

# RECONSTRUCTING FUNCTION FIELDS FROM RATIONAL QUOTIENTS OF MOD- $\ell$ GALOIS GROUPS

ADAM TOPAZ

ABSTRACT. In this paper, we develop the main step in the *global theory* for the mod- $\ell$  analogue of Bogomolov's program in birational anabelian geometry for higher-dimensional function fields over algebraically closed fields. More precisely, we show how to reconstruct a function field  $K$  of transcendence degree  $\geq 5$  over an algebraically closed field, up-to inseparable extensions, from the mod- $\ell$  abelian-by-central Galois group of  $K$  endowed with the collection of mod- $\ell$  rational quotients.

## CONTENTS

1. Introduction	1
2. Milnor K-theory	10
3. Milnor K-theory of Function Fields	13
4. Graded Lattices	18
5. Recovering the Mod- $\ell$ Lattice	20
6. Combinatorial Geometries	24
7. Proof of Theorem B	27
8. The Zassenhauss Filtration and Galois Cohomology	34
9. Proof of Theorem A	39
References	41

## 1. INTRODUCTION

In the early 1990's, BOGOMOLOV [Bog91] introduced a program whose ultimate goal is to reconstruct higher-dimensional function fields over algebraically closed fields from their pro- $\ell$  *abelian-by-central* Galois groups. If successful, this program would go far beyond Grothendieck's birational anabelian geometry, since Bogomolov's program deals with *small* pro- $\ell$  Galois groups and with fields which are purely *geometric* in nature.

In this paper, we consider the *mod- $\ell$  abelian-by-central* variant of Bogomolov's program. The mod- $\ell$  context is fundamentally different than the pro- $\ell$  context, primarily with respect to the *global theory*, because one can no longer use the *fundamental theorem of projective geometry* (see the detailed discussion below). The primary goal of this paper is to develop the *global theory* in the mod- $\ell$  context by using the results of EVANS-HRUSHOVSKI [EH91],

---

*Date:* October 30, 2015.

2010 *Mathematics Subject Classification.* 12F10, 12G05, 12J10, 19D45.

*Key words and phrases.* Anabelian geometry, pro- $\ell$  groups, Galois groups, Milnor K-theory, Galois cohomology, abelian-by-central, global theory, function fields, prime divisors, combinatorial geometry.

This research was supported by NSF postdoctoral fellowship DMS-1304114.

[EH95] and GISMATULLIN [Gis08], which stem from the so-called “group-configuration theorem” in geometric stability theory. The analogy between the fundamental theorem of projective geometry and the work of EVANS-HRUSHOVSKI and GISMATULLIN has been long known to model theorists, and it was also recently noticed in the context of Galois theory by BOGOMOLOV-TSCHINKEL [BT12]. Nevertheless, the present paper seems to be the first to use these results in the context of anabelian geometry in an essential way.

To make Bogomolov’s program into a precise conjecture, we begin by introducing some notation. Throughout the paper we will work with a fixed prime  $\ell$ . In the context of profinite groups, we will tacitly consider only continuous maps and closed subgroups. For a field  $F$ , denote by  $\mathcal{G}_F := \text{Gal}(F(\ell)|F)$  the maximal pro- $\ell$  Galois group of  $F$ . Also, we will let  $F^i$  denote the perfect closure of  $F$ .

Let  $K$  be a function field over an algebraically closed field  $k$ . In this case, consider the following two Galois groups which are constructed from  $\mathcal{G}_K$ , with notation/terminology due to POP [Pop12a]:

- (1)  $\Pi_K^a := \mathcal{G}_K/[\mathcal{G}_K, \mathcal{G}_K]$ , the maximal **pro- $\ell$  abelian** Galois group of  $K$ .
- (2)  $\Pi_K^c := \mathcal{G}_K/[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]$ , the maximal **pro- $\ell$  abelian-by-central** Galois group of  $K$ .

Now let  $L$  be another function field over an algebraically closed field  $l$ . We denote by  $\text{Isom}^i(K, L)$  the collection of isomorphisms  $\phi : K^i \rightarrow L^i$ . Note that any such isomorphism  $\phi$  automatically satisfies  $\phi k = l$ , since  $k$  resp.  $l$  is the set of multiplicatively divisible elements in  $K^i$  resp.  $L^i$ . If  $\text{char } k = p > 0$ , then the Frobenius automorphism  $\text{Frob}_p : K^i \rightarrow K^i$  acts on  $\text{Isom}^i(K, L)$  by composition. In this case we denote by  $\text{Isom}_F^i(K, L)$  the orbits of this action on  $\text{Isom}^i(K, L)$ . If  $\text{char } k = 0$ , then we define  $\text{Isom}_F^i(K, L) := \text{Isom}^i(K, L) = \text{Isom}(K, L)$  to keep the notation consistent.

We will denote by  $\Delta_K$  the kernel of the central extension  $\Pi_K^c \twoheadrightarrow \Pi_K^a$ . Note that both  $\Pi_K^a$  and  $\Delta_K$  are abelian pro- $\ell$  groups, and we will consider them as (additive)  $\mathbb{Z}_\ell$ -modules. For  $\sigma, \tau \in \Pi_K^a$ , we define  $[\sigma, \tau] := \tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}$  where  $\tilde{\sigma}, \tilde{\tau} \in \Pi_K^c$  are some lifts of  $\sigma, \tau$ . Since  $\Pi_K^c \twoheadrightarrow \Pi_K^a$  is a central extension, the element  $[\sigma, \tau] \in \Delta_K$  doesn’t depend on the choice of lifts of  $\sigma, \tau$ , and it is well known that  $[\bullet, \bullet] : \Pi_K^a \times \Pi_K^a \rightarrow \Delta_K$  is  $\mathbb{Z}_\ell$ -bilinear.

We say that an isomorphism  $\phi : \Pi_L^a \rightarrow \Pi_K^a$  is **compatible with  $[\bullet, \bullet]$**  if there exists some isomorphism  $\psi : \Delta_L \rightarrow \Delta_K$  such that  $\psi[\sigma, \tau] = [\phi\sigma, \phi\tau]$  for all  $\sigma, \tau \in \Pi_L^a$ . We denote by  $\text{Isom}^c(\Pi_L^a, \Pi_K^a)$  the collection of isomorphisms  $\phi : \Pi_L^a \rightarrow \Pi_K^a$  which are compatible with  $[\bullet, \bullet]$ . Note that if  $\epsilon \in \mathbb{Z}_\ell^\times$  and  $\phi \in \text{Isom}^c(\Pi_L^a, \Pi_K^a)$ , then we obtain an induced isomorphism  $\epsilon \cdot \phi : \Pi_L^a \rightarrow \Pi_K^a$ , defined by

$$(\epsilon \cdot \phi)(x) = \epsilon \cdot \phi(x) = \phi(\epsilon \cdot x).$$

Since  $[\bullet, \bullet]$  is  $\mathbb{Z}_\ell$ -bilinear, it follows that  $\epsilon \cdot \phi$  is also an element of  $\text{Isom}^c(\Pi_L^a, \Pi_K^a)$ . Thus, we have a canonical left-multiplication action of  $\mathbb{Z}_\ell^\times$  on  $\text{Isom}^c(\Pi_L^a, \Pi_K^a)$ , and we denote the orbits of this action by  $\underline{\text{Isom}}^c(\Pi_L^a, \Pi_K^a)$ .

Since the inclusion  $K \hookrightarrow K^i$  induces an isomorphism  $G_{K^i} \rightarrow G_K$  of absolute Galois groups, we obtain a canonical map  $\text{Isom}^i(K, L) \rightarrow \text{Isom}^c(\Pi_L^a, \Pi_K^a)$ . If  $\text{char } K \neq \ell$ , we therefore also have an induced canonical map

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}^c(\Pi_L^a, \Pi_K^a).$$

Using the notation above, POP [Pop12b] formulated the following conjecture which is a precise “Isom” version of Bogomolov’s program in birational anabelian geometry – see the “Target Result” in loc.cit.

**Conjecture 1** (BOGOMOLOV [Bog91], POP [Pop12b]). *Let  $K|k$  and  $L|l$  be function fields over algebraically closed fields such that  $\text{char } K \neq \ell$  and  $\text{tr. deg}(K|k) \geq 2$ . Then the canonical map*

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}^c(\Pi_L^a, \Pi_K^a)$$

*is a bijection.*

The proof of Conjecture 1 should also give some isomorphism-compatible *group-theoretical recipe* which constructs  $K^i|k$  as fields from  $\Pi_K^c$  as a pro- $\ell$  group. Also, note that the validity of Conjecture 1 would imply that  $K^i|k \cong L^i|l$  as fields if and only if  $\Pi_L^c \cong \Pi_K^c$  as pro- $\ell$  groups. While this conjecture is far from being proven in full generality, it has been settled in the case where  $k$  is the *algebraic closure of a finite field*, by BOGOMOLOV-TSCHINKEL [BT08], [BT11], and separately by POP [Pop12a].

**1.1. The Pro- $\ell$  Strategy.** For readers’ sake, we summarize the general strategy for proving Conjecture 1, as outlined in the introduction of [Pop12b]. We will henceforth refer to this as **The Pro- $\ell$  Strategy**.

For  $K|k$  as in Conjecture 1, we note that  $\mu_{\ell^\infty} \subset K$ . After fixing an isomorphism  $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$  of  $G_K$ -modules, it follows from Kummer theory that one has an isomorphism

$$\text{Hom}(\Pi_K^c, \mathbb{Z}_\ell) = \text{Hom}(\Pi_K^a, \mathbb{Z}_\ell) \cong \widehat{K^\times}$$

where  $\widehat{K^\times}$  denotes the  $\ell$ -adic completion of  $K^\times$ . Next, note that the  $\ell$ -adic completion map  $K^\times \rightarrow \widehat{K^\times}$  has  $k^\times$  as its kernel, so that  $K^\times/k^\times$  can be embedded as a subgroup of  $\widehat{K^\times}$ . Using this observation, **the pro- $\ell$  strategy** for reconstructing  $K$  using  $\Pi_K^c$  has three key steps:

(1) First, determine  $K^\times/k^\times$  as a subset of

$$\text{Hom}(\Pi_K^c, \mathbb{Z}_\ell) = \text{Hom}(\Pi_K^a, \mathbb{Z}_\ell) \cong \widehat{K^\times}.$$

Note that  $K^\times/k^\times$  can be considered as the (infinite-dimensional) projective space, since it is the projectivization  $\mathcal{P}_k(K)$  of  $K$  as a  $k$ -vector space.

- (2) Second, determine the projective lines on  $\mathcal{P}_k(K)$ . Since the multiplicative structure of  $K^\times/k^\times$  is “known” from step (1), it suffices to determine the projective lines of  $\mathcal{P}_k(K)$  which contain  $1 \in K^\times/k^\times$ .
- (3) Third, apply the *Fundamental Theorem of Projective Geometry* (cf. [Art57] Ch. II.10) to  $\mathcal{P}_k(K)$  in order to obtain the structure of  $K$  as a vector space over  $k$ , then use the multiplicative structure of  $K^\times/k^\times$  to recover the multiplicative structure of  $K$ .

As with most other results in anabelian geometry, the strategy to tackle the three key steps above consists of two main parts: *the local theory* and *the global theory*. Some portions of each part are known over an arbitrary algebraically closed field, but one must restrict to the algebraic closure of a finite field for everything to fit together. The following is a brief summary of each part.

*The Pro- $\ell$  Local Theory:* Here the goal is to use  $\Pi_K^c$  in order to recover information about decomposition and inertia subgroups of  $\Pi_K^a$  associated to *divisorial valuations* of  $K|k$  (i.e.

valuations arising from Weil-prime-divisors on normal models of  $K|k$ ), as well as their Parshin-chains. The primary tool in this context is BOGOMOLOV and TSCHINKEL's theory of *commuting-liftable pairs* in pro- $\ell$  abelian-by-central Galois groups [BT02]. Presently, the best one can do over an arbitrary algebraically closed field is to recover the decomposition/inertia subgroups of  $\Pi_K^a$  associated to *quasi-divisorial valuations*; see [Pop10] for the details and for the precise definition of quasi-divisorial valuations. Nevertheless, over the algebraic closure of a finite field, quasi-divisorial valuations are precisely the divisorial valuations.

*The Pro- $\ell$  Global Theory:* Using the local theory as an input, the global theory tackles the three key steps of the pro- $\ell$  strategy, by further using the collection of *rational quotients* of  $\Pi_K^a$ . This main step in the pro- $\ell$  global theory is the Main Theorem of [Pop12b]. See loc.cit. for the details about pro- $\ell$  rational quotients, but note also that we define the mod- $\ell$  analogue of a rational quotient in §1.4. From here, the main problem is to reconstruct these rational quotients using the given group-theoretical data. This is accomplished over the algebraic closure of a finite field in [Pop12a].

The present paper considers the *mod- $\ell$  analogue* of the context above (see the precise notation introduced below). Roughly speaking, this corresponds to replacing  $\Pi_K^a$  with

$$\mathcal{G}_K^a := \frac{\mathcal{G}_K}{[\mathcal{G}_K, \mathcal{G}_K] \cdot (\mathcal{G}_K)^\ell} = \frac{\Pi_K^a}{(\Pi_K^a)^\ell}.$$

Dually by Kummer theory, this corresponds to replacing  $\widehat{K^\times}$  by  $K^\times/\ell$ . Namely, the objects in the mod- $\ell$  context are essentially obtained by modding out the corresponding pro- $\ell$  objects by  $\ell$ -th powers. In particular, *the mod- $\ell$  context generalizes the pro- $\ell$  context*.

The fundamental problem in the mod- $\ell$  context is that the pro- $\ell$  strategy, using the three key steps above, fails from the very beginning. This is precisely because  $K^\times/\ell$  contains no apparent geometric object on which one can apply results concerning projective geometry over  $k$ . The main goal of this paper is to overcome this fundamental difficulty, and to develop a mod- $\ell$  version of the *global theory*. We now discuss the notation/context for the mod- $\ell$  situation in detail.

**1.2. The mod- $\ell$  analogue.** We begin by introducing the mod- $\ell$  analogue of the notation above in order to state the mod- $\ell$  analogue of Conjecture 1. We first recall the first two non-trivial terms in the mod- $\ell$  *Zassenhauss* filtration of a pro- $\ell$  group  $\mathcal{G}$ :

- (1)  $\mathcal{G}^{(2)} := [\mathcal{G}, \mathcal{G}] \cdot \mathcal{G}^\ell$ .
- (2) If  $\ell \neq 2$ , then  $\mathcal{G}^{(3)} := [\mathcal{G}, \mathcal{G}^{(2)}] \cdot \mathcal{G}^\ell$ .
- (3) If  $\ell = 2$ , then  $\mathcal{G}^{(3)} := [\mathcal{G}, \mathcal{G}^{(2)}] \cdot (\mathcal{G}^{(2)})^\ell$ .

We define  $\mathcal{G}^a := \mathcal{G}/\mathcal{G}^{(2)}$  and  $\mathcal{G}^c := \mathcal{G}/\mathcal{G}^{(3)}$ , and we note that  $\mathcal{G}^c \twoheadrightarrow \mathcal{G}^a$  is a central extension.

Suppose that  $K$  is a function field over an algebraically closed field  $k$ , and recall that  $\mathcal{G}_K$  denotes the maximal pro- $\ell$  Galois group of  $K$ . In this case, we will denote the kernel of  $\mathcal{G}_K^c \twoheadrightarrow \mathcal{G}_K^a$  by  $\mathfrak{Z}_K$ , and we note that  $\mathcal{G}_K^a$  and  $\mathfrak{Z}_K$  are both  $\ell$ -elementary abelian. We will consider both  $\mathcal{G}_K^a$  and  $\mathfrak{Z}_K$  as (additive)  $\mathbb{Z}/\ell$ -modules. In comparison with the pro- $\ell$  context, we note that one has

$$\frac{\Pi_K^c}{(\Pi_K^c)^{(2)}} = \frac{\Pi_K^a}{(\Pi_K^a)^{(2)}} = \mathcal{G}_K^a, \quad \frac{\Pi_K^c}{(\Pi_K^c)^{(3)}} = \mathcal{G}_K^c.$$

Hence, our mod- $\ell$  context indeed generalizes the pro- $\ell$  context.

Similarly to the pro- $\ell$  context, for  $\sigma, \tau \in \mathcal{G}_K^a$ , we define  $[\sigma, \tau] := \tilde{\sigma}^{-1} \tilde{\tau}^{-1} \tilde{\tau} \tilde{\sigma}$  where  $\tilde{\sigma}, \tilde{\tau} \in \mathcal{G}_K^c$  are some lifts of  $\sigma, \tau$ . Since  $\mathcal{G}_K^c \rightarrow \mathcal{G}_K^a$  is a central extension, we again see that  $[\sigma, \tau] \in \mathfrak{Z}_K$  doesn't depend on the choice of lifts of  $\sigma, \tau$ , and it is again well-known that  $[\bullet, \bullet] : \mathcal{G}_K^a \times \mathcal{G}_K^a \rightarrow \mathfrak{Z}_K$  is  $\mathbb{Z}/\ell$ -bilinear. Finally, we denote by  $\mathfrak{Z}_K^0$  the (closed) subgroup of  $\mathfrak{Z}_K$  which is generated by elements of the form  $[\sigma, \tau]$  as  $\sigma, \tau \in \mathcal{G}_K^a$  vary. If  $\ell \neq 2$ , then it follows from the definition of the mod- $\ell$  Zassenhauss filtration that  $\mathfrak{Z}_K^0 = \mathfrak{Z}_K$ . On the other hand, if  $\ell = 2$ , then  $\mathfrak{Z}_K^0$  might be properly contained in  $\mathfrak{Z}_K$ .

Let  $L$  be another function field over an algebraically closed field  $l$ . We say that an isomorphism  $\phi : \mathcal{G}_L^a \rightarrow \mathcal{G}_K^a$  is **compatible with  $[\bullet, \bullet]$**  if there exists some isomorphism  $\psi : \mathfrak{Z}_L^0 \rightarrow \mathfrak{Z}_K^0$  such that  $\psi[\sigma, \tau] = [\phi\sigma, \phi\tau]$  for all  $\sigma, \tau \in \mathcal{G}_L^a$ . We define  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  to be the collection of isomorphisms  $\mathcal{G}_L^a \rightarrow \mathcal{G}_K^a$  which are compatible with  $[\bullet, \bullet]$ . If  $\epsilon \in (\mathbb{Z}/\ell)^\times$  and  $\phi \in \text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ , then we obtain an induced isomorphism  $\epsilon \cdot \phi : \mathcal{G}_L^a \rightarrow \mathcal{G}_K^a$ , defined by

$$(\epsilon \cdot \phi)(x) = \epsilon \cdot \phi(x) = \phi(\epsilon \cdot x).$$

Since  $[\bullet, \bullet]$  is  $\mathbb{Z}/\ell$ -bilinear, it follows that  $\epsilon \cdot \phi$  is also an element of  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ . Thus, we obtain a canonical action of  $(\mathbb{Z}/\ell)^\times$  on  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ , and we denote the orbits of this action by  $\underline{\text{Isom}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ .

Since  $K \hookrightarrow K^i$  induces an isomorphism  $G_{K^i} \rightarrow G_K$  of absolute Galois groups, we obtain a canonical map  $\text{Isom}^i(K, L) \rightarrow \text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ . If  $\text{char } K \neq \ell$ , we therefore also obtain an induced canonical map

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a).$$

With this notation, we can formulate the following mod- $\ell$  analogue of Conjecture 1.

**Conjecture 2.** *Let  $K|k$  and  $L|l$  be function fields over algebraically closed fields such that  $\text{char } K \neq \ell$  and  $\text{tr. deg}(K|k) \geq 2$ . Then the canonical map*

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$$

*is a bijection.*

The proof of Conjecture 2 should also provide an isomorphism-compatible group-theoretical recipe which constructs  $K^i|k$  as fields from  $\mathcal{G}_K^c$  as a pro- $\ell$  group. Moreover, note that the validity of Conjecture 2 would imply that  $K^i|k \cong L^i|l$  as fields if and only if  $\mathcal{G}_L^c \cong \mathcal{G}_K^c$  as pro- $\ell$  groups. As mentioned above, we note that Conjecture 2 can be used when considering Conjecture 1, because the canonical map  $\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  considered in Conjecture 2 factors through the map  $\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}^c(\Pi_L^a, \Pi_K^a)$  from Conjecture 1. Thus, Conjecture 2 reduces Conjecture 1 to proving that the map

$$\underline{\text{Isom}}^c(\Pi_L^a, \Pi_K^a) \rightarrow \underline{\text{Isom}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$$

is injective, which we expect would follow from the methods in this paper.

**1.3. The Mod- $\ell$  Strategy.** Until now, no strategy has even been formulated to tackle Conjecture 2. Nevertheless, it is natural to expect that such a mod- $\ell$  strategy might involve two parts – a *local theory* and a *global theory* – similarly to the pro- $\ell$  context. While the mod- $\ell$  local theory is essentially understood, it was the mod- $\ell$  global theory which posed a significant hurdle. The following describes what is known in the mod- $\ell$  situation.

*The Mod- $\ell$  Local Theory:* The mod- $\ell$  version of the local theory is understood just as well as the pro- $\ell$  local theory. More precisely, POP [Pop11] shows, using similar methods to the pro- $\ell$  version in [Pop10], that minimized inertia/decomposition subgroups of  $\mathcal{G}_K^a$  associated to Parshin-chains of quasi-divisorial valuations can be determined from the group-theoretical structure of  $\mathcal{G}_K^c$ . The main difference between the two approaches is that the pro- $\ell$  version uses Bogomolov and Tschinkel’s theory of commuting-liftable pairs [BT02], while the mod- $\ell$  version requires the mod- $\ell$  version of the theory of commuting-liftable pairs which was developed by the author in [Top14a] and/or [Top14b].

*The Mod- $\ell$  Global Theory:* Until now, nothing was known concerning a possible mod- $\ell$  global theory. This is primarily because there is no apparent “geometric” object which can be obtained from the given mod- $\ell$  Galois-theoretical data. More precisely, an analog of the pro- $\ell$  strategy fails from the very beginning in the mod- $\ell$  context, since there is no apparent subset of  $\text{Hom}(\mathcal{G}_K^a, \mathbb{Z}/\ell) \cong K^\times/\ell$  on which one can hope to apply results concerning projective geometry over  $k$ .

Despite this fundamental difficulty, in this paper, we develop a mod- $\ell$  *global theory* for higher-dimensional function fields. Namely, we prove the mod- $\ell$  analogue of the Main Theorem of [Pop12b], for function fields of transcendence degree  $\geq 5$ . More precisely, we show how to recover the function field  $K|k$ , up-to inseparable extensions, from  $\mathcal{G}_K^c$  together with the *rational quotients* of  $\mathcal{G}_K^a$ , which will be explicitly defined in §1.4. Thus, our main theorem reduces Conjecture 2 in transcendence degree  $\geq 5$  to the problem of determining these rational quotients of  $\mathcal{G}_K^a$  using  $\mathcal{G}_K^c$ .

Our approach uses a modern *analogue* of the fundamental theorem of projective geometry, which stems from the so-called “group-configuration theorem” in geometric stability theory. Much like the fundamental theorem of projective geometry, which determines a field and a vector space from the associated projective space and its lines, the analogous theorem which we use here determines a field and a field extension using the so-called “combinatorial geometry” associated to relative algebraic closure. This analogue of the fundamental theorem of projective geometry was originally developed by EVANS-HRUSHOVSKI [EH91], [EH95] for extensions of algebraically closed fields, and was later generalized to arbitrary extensions of fields by GISMATULLIN [Gis08]. Thus, the main strategy in this paper is to construct this combinatorial geometry using the given Galois group  $\mathcal{G}_K^c$  endowed with the collection of rational quotients of  $\mathcal{G}_K^a$ .

The main reason that our main theorems require the assumption that  $\text{tr. deg} \geq 5$  is because we use the results of [Gis08], which in turn uses the results of [EH95] where this assumption originally appeared. As mentioned above, loc.cit. uses the “group-configuration theorem” from geometric stability theory. The assumption that  $\text{tr. deg} \geq 5$  is required in loc.cit. for a technical step which determines which group-configurations arise from the multiplicative group resp. the additive group of  $K$ . In fact, it is mentioned on the first page of [EH95] that similar results are expected to hold true for  $\text{tr. deg} \geq 3$ , although this is still open.

On the other hand, all of the results of the present paper leading up to the proof of our main theorems work when  $\text{tr. deg} \geq 4$ , and most of them actually work for arbitrary transcendence degree; see the results in §5 where we first put an explicit assumption on the transcendence degree. We only restrict to  $\text{tr. deg} \geq 5$  when we finally use [Gis08]. Similarly to EVANS-HRUSHOVSKI [EH95], we actually expect our results to be true for  $\text{tr. deg} \geq 3$ .



Finally, we note that the similarity between the fundamental theorem of projective geometry and the results of EVANS-HRUSHOVSKI and GISMATULLIN has been long known to model theorists; see e.g. the MathSciNet review for [EH95], which was written by PILLAY. This similarity was also recently noticed by BOGOMOLOV-TSCHINKEL [BT12]. However, the work of BOGOMOLOV-TSCHINKEL doesn't use the results of EVANS-HRUSHOVSKI and GISMATULLIN in any meaningful way, since the fundamental theorem of projective geometry always applies in their contexts. Thus, the present paper seems to be the first to use combinatorial geometries for applications in anabelian geometry in an essential way.

**1.4. Main Theorem (Galois variant).** Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ . Suppose that  $F$  is a subextension of  $K|k$  which is algebraically closed in  $K$ . Then by Kummer theory, the associated map of abelian pro- $\ell$  Galois groups  $\mathcal{G}_K^a \twoheadrightarrow \mathcal{G}_F^a$  is surjective. For a (closed) subgroup  $H$  of  $\mathcal{G}_K^a$ , we say that the group-theoretical quotient  $\pi_H : \mathcal{G}_K^a \twoheadrightarrow \mathcal{G}_K^a/H$  is a **rational quotient** of  $\mathcal{G}_K^a$  if  $H$  is the kernel of the surjective map  $\mathcal{G}_K^a \twoheadrightarrow \mathcal{G}_F^a$  associated to some relatively algebraically closed subextension  $F$  of  $K|k$ , such that  $\text{tr. deg}(F|k) = 1$  and  $F = k(t)$  for some  $t \in K$ . The collection of rational quotients of  $\mathcal{G}_K^a$  will be denoted by  $\mathfrak{R}_{\text{rat}}(K|k)$ .

If  $L$  is another function field over an algebraically closed field  $l$  such that  $\text{char } l \neq \ell$ , we say that an isomorphism  $\phi : \mathcal{G}_L^a \rightarrow \mathcal{G}_K^a$  is **compatible with  $\mathfrak{R}_{\text{rat}}$**  if  $\phi$  induces a bijection  $\mathfrak{R}_{\text{rat}}(L|l) \rightarrow \mathfrak{R}_{\text{rat}}(K|k)$ . We denote by  $\text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  the collection of isomorphisms  $\phi : \mathcal{G}_L^a \rightarrow \mathcal{G}_K^a$  which are compatible with  $[\bullet, \bullet]$  and with  $\mathfrak{R}_{\text{rat}}$ . Thus  $\text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  is a subset of  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ . Moreover, the action of  $(\mathbb{Z}/\ell)^\times$  on  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  restricts to an action on  $\text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ . We denote by  $\underline{\text{Isom}}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  the orbits of this action on  $\text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ . Furthermore, we note that the image of the canonical map  $\text{Isom}^i(K, L) \rightarrow \text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  lands in the subset  $\text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$ . Thus, we obtain an induced canonical map

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a).$$

We are now prepared to state the main theorem of the paper, which is precisely the mod- $\ell$  analogue of the Main Theorem from [Pop12b] in transcendence degree  $\geq 5$ .

**Theorem A** (Galois variant). *Let  $K|k$  and  $L|l$  be function fields over algebraically closed fields such that  $\text{char } K \neq \ell$  and  $\text{tr. deg}(K|k) \geq 5$ . Then the following hold:*

- (1) *There is an isomorphism-compatible group-theoretical recipe which constructs  $K^i|k$  as fields from  $\mathcal{G}_K^c$  as a pro- $\ell$  group together with  $\mathfrak{R}_{\text{rat}}(K|k)$ , the collection of rational quotients of  $\mathcal{G}_K^a$ .*
- (2) *If  $\underline{\text{Isom}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  is non-empty, then  $\text{char } L \neq \ell$ , and the canonical map*

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$$

*is a bijection. In particular,  $K|k$  and  $L|l$  are isomorphic, up-to inseparable extensions, if and only if there is an isomorphism  $\mathcal{G}_L^c \xrightarrow{\cong} \mathcal{G}_K^c$  such that the induced isomorphism  $\mathcal{G}_L^a \xrightarrow{\cong} \mathcal{G}_K^a$  is compatible with  $\mathfrak{R}_{\text{rat}}$ .*

In particular, Theorem A reduces Conjecture 2, for a function field  $K|k$  of transcendence degree  $\geq 5$ , to reconstructing the collection  $\mathfrak{R}_{\text{rat}}(K|k)$  of mod- $\ell$  rational quotients in a group-theoretical way from  $\mathcal{G}_K^c$ . Currently, this step remains open. Nevertheless, we expect that this reconstruction is indeed possible, based on the fact that, *over the algebraic closure of a finite field*, POP [Pop12a] reconstructs the *pro- $\ell$  rational quotients* using  $\Pi_K^c$ .

**1.5. Main Theorem (Minor variant).** The majority of the paper is devoted to proving an analogue of Theorem A which deals with  $k_*^M(K)$ , the mod- $\ell$  Milnor K-ring of  $K$ , instead of  $\mathcal{G}_K^c$ . The definition of  $k_*^M(K)$  is reviewed in §2, although we recall now that  $k_1^M(K) = K^\times/\ell$ .

It is important to note that results which reconstruct function fields using Milnor K-theory have been previously developed by BOGOMOLOV-TSCHINKEL [BT09]. The main difference between the results of loc.cit. and our mod- $\ell$  context, is that [BT09] works with the *Milnor K-ring modulo divisible elements*, denoted by  $\overline{K}_*^M(K)$ . On the other hand, Theorem B below deals with the *mod- $\ell$  Milnor K-ring*  $k_*^M(K)$ , which is a fairly small quotient of  $\overline{K}_*^M(K)$ ; more precisely, one has  $k_*^M(K) = \overline{K}_*^M(K)/\ell$ .

For  $K$  a function field over an algebraically closed field  $k$ , we note that one has

$$\overline{K}_1^M(K) = K^\times/k^\times.$$

In particular, the set  $K^\times/k^\times$  underlying the projective space  $\mathcal{P}_k(K)$  is given. With this observation, the strategy in [BT09] is to first recover the collection of projective lines, and to ultimately apply the fundamental theorem of projective geometry on  $\mathcal{P}_k(K)$ . It is therefore unlikely that a similar strategy will work when replacing  $\overline{K}_*^M(K)$  with  $k_*^M(K)$  as we have done in Theorem B below, similarly to the reason that the pro- $\ell$  strategy doesn't apply in the mod- $\ell$  context (see §1.3).

To state the “Milnor Variant” of our main theorem, we first recall that Kummer theory yields a canonical perfect pairing

$$\mathcal{G}_K^a \times k_1^M(K) \rightarrow \mu_\ell.$$

In the case where  $K$  is a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ , we say that a subgroup  $A$  of  $k_1^M(K)$  is a **rational subgroup** if there exists a subextension  $F$  of  $K|k$  such that  $F$  is algebraically closed in  $K$ ,  $\text{tr. deg}(F|k) = 1$ ,  $F = k(t)$  for some  $t \in K$ , and  $A$  is the image of the canonical map  $F^\times \rightarrow k_1^M(K)$ . The collection of all rational subgroups of  $k_1^M(K)$  will be denoted by  $\mathfrak{S}_{\text{rat}}^1(K|k)$ . Furthermore, note that the Kummer pairing above yields a one-to-one correspondence between  $\mathfrak{R}_{\text{rat}}(K|K)$  and  $\mathfrak{S}_{\text{rat}}^1(K|k)$ , since rational quotients of  $\mathcal{G}_K^a$  are Kummer-dual to rational subgroups of  $k_1^M(K)$ .

If  $L$  is another function field over an algebraically closed field  $l$  such that  $\text{char } l \neq \ell$ , then we say that an isomorphism  $\phi : k_1^M(K) \rightarrow k_1^M(L)$  is **compatible with  $k_2^M$**  if the induced map  $\phi^{\otimes 2} : k_1^M(K)^{\otimes 2} \rightarrow k_1^M(L)^{\otimes 2}$  descends to an isomorphism  $k_2^M(K) \rightarrow k_2^M(L)$ . We denote by  $\text{Isom}^M(k_1^M(K), k_1^M(L))$  the collection of isomorphisms  $\phi : k_1^M(K) \rightarrow k_1^M(L)$  which are compatible with  $k_2^M$ . Since the inclusion  $K \hookrightarrow K^i$  induces an isomorphism of mod- $\ell$  Milnor K-rings  $k_*^M(K) \xrightarrow{\cong} k_*^M(K^i)$  (see Fact 2.1), we obtain a canonical map  $\text{Isom}^i(K, L) \rightarrow \text{Isom}^M(k_1^M(K), k_1^M(L))$ .

We say that an isomorphism  $\phi : k_1^M(K) \rightarrow k_1^M(L)$  is **compatible with  $\mathfrak{S}_{\text{rat}}^1$**  if  $\phi$  induces a bijection  $\mathfrak{S}_{\text{rat}}^1(K|k) \rightarrow \mathfrak{S}_{\text{rat}}^1(L|l)$ . We denote by  $\text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  the collection of isomorphisms  $\phi : k_1^M(K) \rightarrow k_1^M(L)$  which are compatible with  $k_2^M$  and with  $\mathfrak{S}_{\text{rat}}^1$ . In particular,  $\text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  is a subset of  $\text{Isom}^M(k_1^M(K), k_1^M(L))$ . Furthermore, it's easy to see that the image of the canonical map  $\text{Isom}^i(K, L) \rightarrow \text{Isom}^M(k_1^M(K), k_1^M(L))$  is contained in  $\text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$ .



If  $\phi \in \text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  and  $\epsilon \in (\mathbb{Z}/\ell)^\times$ , then we obtain an induced isomorphism  $\epsilon \cdot \phi : k_1^M(K) \rightarrow k_1^M(L)$ , defined by

$$(\epsilon \cdot \phi)(x) = \phi(x)^\epsilon = \phi(x^\epsilon),$$

where we denote  $k_1^M(K) = K^\times/\ell$  resp.  $k_1^M(L) = L^\times/\ell$  multiplicatively. Since  $k_*^M(K)$  and  $k_*^M(L)$  are  $\mathbb{Z}/\ell$ -algebras, it follows that  $\epsilon \cdot \phi$  is also an element of  $\text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$ . Thus, we have a canonical action of  $(\mathbb{Z}/\ell)^\times$  on  $\text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  whose orbits we denote by  $\underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$ . In particular, we obtain an induced map

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$$

which is the mod- $\ell$  Milnor K-ring analogue of the map  $\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  considered in Theorem A. The main goal of the paper is to prove the following “Milnor variant” of Theorem A.

**Theorem B** (Milnor variant). *Let  $K|k$  and  $L|l$  be function fields over algebraically closed fields, such that  $\text{char } K \neq \ell$ ,  $\text{char } L \neq \ell$ , and  $\text{tr. deg}(K|k) \geq 5$ . Then the following hold:*

- (1) *There is an isomorphism-compatible group-theoretical recipe which constructs  $K^i|k$  as fields from the following data  $\mathcal{K}_{\text{rat}}^M(K|k)$ :*
  - *The groups  $k_1^M(K)$  and  $k_2^M(K)$ .*
  - *The multiplication map  $k_1^M(K) \otimes k_1^M(K) \rightarrow k_2^M(K)$ .*
  - *The collection  $\mathfrak{G}_{\text{rat}}^1(K|k)$  of rational subgroups of  $k_1^M(K)$ .*
- (2) *The canonical map*

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$$

*is a bijection. In particular,  $K|k$  and  $L|l$  are isomorphic, up-to inseparable extensions, if and only if there is an isomorphism  $k_1^M(K) \xrightarrow{\cong} k_1^M(L)$  which is compatible with  $k_2^M$  and with  $\mathfrak{G}_{\text{rat}}^1$ .*

**1.6. A guide through the paper.** The following is a description of the various sections of this paper, and a summary of the proofs of the main theorems:

- (1) In §2, we recall the definition of the Milnor K-ring  $K_*^M(K)$  of a field  $K$  as well as its mod- $\ell$  version  $k_*^M(K)$ . We also recall some basic properties of the Milnor K-ring, especially with respect to *tame symbols*.
- (2) In §3, we prove some vanishing/non-vanishing results in mod- $\ell$  Milnor K-theory of a function field  $K$  over an algebraically closed field  $k$ . The “vanishing” result states that  $k_s^M(K) = 0$  whenever  $s > \text{tr. deg}(K|k) =: d$ . This follows from the fact that  $K$  has  $\ell$ -cohomological dimension  $d$ , combined with the Bloch-Kato conjecture, which is now a theorem of VOEVODSKY-ROST et al. [Voe11], [Ros98], [Wei09]. On the other hand, the “non-vanishing” results assert that there are “many” elements  $x_1, \dots, x_r \in k_1^M(K)$  such that  $\{x_1, \dots, x_r\} \neq 0$  in  $k_r^M(K)$ , for  $r \leq d$ , and that these elements can generally be found in relatively algebraically closed subextensions of  $K|k$ .
- (3) In §4 we recall the definition of a *graded lattice* and give the main example considered in this paper: the graded lattice  $\mathbb{G}^*(K|k)$  associated to relative algebraic closure in the field extension  $K|k$ . In this section we also use the results of §3 to prove that an isomorphic copy of this graded lattice, denoted  $\mathfrak{G}^*(K|k)$ , can be found inside the lattice of subgroups of  $K^\times/\ell = k_1^M(K)$ , in the context of the main theorems.

- (4) The key propositions required to prove the main theorems are found in §5. Namely, under the assumptions/notation of our main theorems, we show how to reconstruct  $\mathfrak{G}^*(K|k)$ , as a subset of the lattice of subgroups of  $k_1^M(K)$ , using  $k_*^M(K)$  along with  $\mathfrak{G}_{\text{rat}}^1(K|k)$ .
- (5) In §6, we recall the standard construction which produces a set with a closure operation from a graded lattice. When applied to the graded lattice  $\mathbb{G}^*(K|k)$ , this construction produces the combinatorial geometry  $\mathbb{G}(K|k)$  which was considered in [EH91], [EH95], and [Gis08]. In this section we also recall the main result of loc.cit. which reconstructs  $K^i|k$  using the combinatorial geometry  $\mathbb{G}(K|k)$ ; this theorem can be seen as the appropriate analogue of the fundamental theorem of projective geometry which applies in this situation.
- (6) Theorem B is proved in §7. Some extra work is required to prove the bijectivity of the map  $\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  considered in Theorem B(2).
- (7) Finally, in §8, we recall the cohomological framework that allows us to translate between Theorems A and B. These cohomological results can be seen as a group-theoretical reformulation of the Merkurjev-Suslin Theorem [MS82]. We conclude the paper by completing the proof of Theorem A in §9.

**Acknowledgments.** The author warmly thank Florian Pop and Thomas Scanlon for numerous technical discussions concerning the topics in this paper. The author also thanks Martin Hils and James Freitag for several helpful discussions. The manuscript was written during the MSRI semester on Model Theory, Arithmetic Geometry and Number theory in the spring of 2014. The author thanks MSRI and the organizers of this semester for their hospitality and for an excellent research environment. The author also thanks the referee for his/her extremely useful comments which helped improve the paper in many ways.

## 2. MILNOR K-THEORY

Let  $K$  be an arbitrary field. We recall that the  $n$ -th **Milnor K-group** of  $K$  is defined as follows:

$$K_n^M(K) := \frac{(K^\times)^{\otimes n}}{\langle a_1 \otimes \cdots \otimes a_n : \exists i < j, a_i + a_j = 1 \rangle}.$$

The tensor product makes  $K_*^M(K) := \bigoplus_{n \geq 0} K_n^M(K)$  into a graded-commutative ring with  $K_0^M(K) = \mathbb{Z}$ , and we denote the product in this ring by  $\{\bullet, \dots, \bullet\}$ .

We will use the fairly standard notation  $k_n^M(K) := K_n^M(K)/\ell$  for the **mod- $\ell$  Milnor K-groups** of  $K$ . Note that the tensor product also makes  $k_*^M(K) := \bigoplus_{n \geq 0} k_n^M(K)$  into a graded-commutative ring with  $k_0^M(K) = \mathbb{Z}/\ell$ . We will abuse the notation and denote the product in  $k_*^M(K)$  also by  $\{\bullet, \dots, \bullet\}$ .

It is clear from the definition that both  $K_*(\bullet)$  and  $k_*(\bullet)$  are functors. For an embedding of fields  $\iota : K \hookrightarrow L$ , we denote by  $\iota_*$  the induced homomorphism  $K_*^M(K) \rightarrow K_*^M(L)$  and/or  $k_*^M(K) \rightarrow k_*^M(L)$ .

If  $L|K$  is a finite extension, we recall that we have a homomorphism  $N_{L|K} : K_*^M(L) \rightarrow K_*^M(K)$  of abelian groups called the **norm**, and that this map agrees with the usual field norm  $N_{L|K} : L^\times \rightarrow K^\times$  in degree 1. The main property of this map which we will use is that the composition  $N_{L|K} \circ \iota_* : K_*^M(K) \rightarrow K_*^M(K)$  is precisely multiplication by  $[L : K]$  (cf. [GS06] Remark 7.3.1). Using this, we obtain the following fact which will be useful in reducing several of our arguments involving finite extensions to the separable case.

**Fact 2.1.** *Suppose that  $\iota : K \hookrightarrow L$  is a purely inseparable finite extension of fields of characteristic different from  $\ell$ . Then the canonical map  $\iota_* : k_*^M(K) \rightarrow k_*^M(L)$  is an isomorphism.*

*Proof.* Let  $p := \text{char } K$  and note that  $\ell$  doesn't divide  $[L : K]$ . From this we see that  $\iota_*$  is injective, since  $N_{L|K} \circ \iota_*$  is multiplication by  $[L : K]$  which is invertible in  $\mathbb{Z}/\ell$ . Moreover, since  $L|K$  is finite and purely inseparable, there exists some  $m \geq 0$  such that  $L \subset K^{1/p^m}$ . If  $\eta \in \ker(k_*^M(L) \rightarrow k_*^M(K^{1/p^m}))$ , then there exists a finite subextension  $L'$  of  $K^{1/p^m}|L$  such that  $\eta \in \ker(k_*^M(L) \rightarrow k_*^M(L'))$ . Since  $L'|L$  is purely inseparable, the argument above implies that  $\eta = 0$ . Namely, the canonical map  $k_*^M(L) \rightarrow k_*^M(K^{1/p^m})$  is injective as well.

On the other hand, the canonical map  $k_*^M(K) \rightarrow k_*^M(K^{1/p^m})$  is an *isomorphism* since  $p$  is invertible in  $\mathbb{Z}/\ell$ . Finally, the inclusion  $K \hookrightarrow K^{1/p^m}$  factors through  $L \hookrightarrow K^{1/p^m}$ , and it follows that the map  $\iota_* : k_*^M(K) \rightarrow k_*^M(L)$  is surjective. We conclude that  $\iota_* : k_*^M(K) \rightarrow k_*^M(L)$  is indeed an isomorphism.  $\square$

**2.1. Milnor dimension.** Let  $K$  be an arbitrary field and let  $S$  be a subset of  $k_1^M(K)$ . Define the **mod- $\ell$  Milnor dimension** of  $S$  in  $k_*^M(K)$ , denoted  $\dim_K^M(S)$ , to be the unique element of  $\{0, 1, \dots, \infty\}$  which satisfies the following property: For all positive integers  $d$ , one has  $\dim_K^M(S) \geq d$  if and only if there exist  $s_1, \dots, s_d \in S$  such that  $\{s_1, \dots, s_d\} \neq 0$  in  $k_d^M(K)$ .

For a non-negative integer  $r \geq 0$ , we define  $\mathfrak{M}^r(K)$  to be the (possibly empty) collection of subgroups of  $k_1^M(K)$  which are *maximal* among subgroups  $B$  of  $k_1^M(K)$  such that  $\dim_K^M(B) = r$ . In particular, the distinct elements of  $\mathfrak{M}^r(K)$  are non-comparable as subgroups of  $k_1^M(K)$ .

By Zorn's lemma, if there exists some subgroup  $A_0$  of  $k_1^M(K)$  such that  $\dim_K^M(A_0) = r$ , then  $\mathfrak{M}^r(K)$  is non-empty. Indeed, suppose that  $(A_i)_i$  is a chain of subgroups of  $k_1^M(K)$  such that  $\dim_K^M(A_i) = r$  for all  $i$ , and let  $A = \bigcup_i A_i$  be the union of the  $A_i$  in  $k_1^M(K)$ . Then it easily follows from the definition that  $A$  is also a subgroup of  $k_1^M(K)$  such that  $\dim_K^M(A) = r$ .

**2.2. Valued fields and tame symbols.** Let  $(K, v)$  be a valued field. We will denote the associated value group by  $vK$ , the residue field by  $Kv$ , the valuation ring by  $\mathcal{O}_v$ , and the valuation ideal by  $\mathfrak{m}_v$ . In certain situations where we wish to keep  $K$  out of the notation, we will use the notation  $\Gamma_v$  for the value group of  $v$  and/or  $\kappa(v)$  for the residue field. Moreover, we will generally denote the canonical map  $\mathcal{O}_v \rightarrow Kv = \kappa(v)$  by  $x \mapsto \bar{x}$ . Lastly, the group  $\mathcal{O}_v^\times$  of  $v$ -units will be denoted by  $U_v$ .

Recall that  $(K, v)$  is called a **discretely valued field** (and/or  $v$  is a **discrete valuation**) provided that  $v$  is a valuation of  $K$  such that  $vK = \mathbb{Z}$ . If  $(K, v)$  is such a discretely valued field, we obtain a homomorphism  $\{\bullet\}_v : K_{n+1}^M(K) \rightarrow K_n^M(Kv)$  for each  $n$ , called the **tame symbol associated to  $v$** , which is uniquely defined by the condition (cf. [GS06] Proposition 7.1.4):

$$(2.1) \quad \{\pi, u_1, \dots, u_n\}_v = \{\bar{u}_1, \dots, \bar{u}_n\}$$

for any element  $\pi \in K^\times$  such that  $v(\pi) = 1$ , and  $v$ -units  $u_1, \dots, u_n \in U_v$ . In particular, note that the tame symbol  $K^\times = K_1^M(K) \rightarrow K_0^M(Kv) = \mathbb{Z}$  in degree 1 is precisely the homomorphism  $v : K^\times \rightarrow \mathbb{Z}$ . Of course, the tame symbol induces homomorphisms  $k_{n+1}^M(K) \rightarrow k_n^M(Kv)$  on mod- $\ell$  Milnor K-theory, which we also denote by  $\{\bullet\}_v$ .

The tame symbol behaves functorially in field extensions, up-to multiplication by the ramification index, as follows. Suppose that  $\iota : (K, v) \hookrightarrow (L, w)$  is a finite extension of discretely valued fields. Let  $e = e(w|v)$  be the ramification index of  $w|v$ ; in other words,

$e := [wL : vK] = w(\pi)$  for an element  $\pi \in K^\times$  such that  $v(\pi) = 1$ . Using equation (2.1), it is easy to see that the following diagram commutes:

$$\begin{array}{ccc} K_{*+1}^M(K) & \xrightarrow{\{\bullet\}_v} & K_*^M(Kv) \\ \downarrow \iota_* & & \downarrow e \cdot \iota_* \\ K_{*+1}^M(L) & \xrightarrow{\{\bullet\}_w} & K_*^M(Lw) \end{array}$$

By tensoring this diagram with  $\mathbb{Z}/\ell$ , we obtain a similar commutative diagram for  $k_*^M$ .

**2.3. Parshin-chains.** Let  $K$  be a field. A **Parshin-chain** of length  $r$  on  $K$  is an ordered collection of valuations  $\mathbf{v} = (v_1, \dots, v_r)$  where each term is a valuation on the residue field of the previous one:

- (1)  $v_1$  is a valuation on  $K$ .
- (2)  $v_{i+1}$  is a valuation on  $\kappa(v_i)$  for all  $i = 1, \dots, r-1$ .

For a Parshin-chain  $\mathbf{v}$  as above, we will write  $\mathbf{v}^\circ := v_r \circ \dots \circ v_1$  for the valuation theoretic composition of the terms of  $\mathbf{v}$ . Thus,  $\mathbf{v}^\circ$  is a valuation on  $K$ . The residue field of  $\mathbf{v}$ , denoted  $K\mathbf{v}$  or  $\kappa(\mathbf{v})$ , is defined to be  $K\mathbf{v}^\circ$ , the residue field of  $\mathbf{v}^\circ$ . Note that  $K\mathbf{v}$  is precisely  $\kappa(v_r)$ , the residue field of  $v_r$  where  $r$  is the length of  $\mathbf{v}$ . Similarly, the group of units of  $\mathbf{v}$ , denoted  $U_{\mathbf{v}}$ , is defined to be  $U_{\mathbf{v}^\circ}$ , the units of  $\mathbf{v}^\circ$ .

Suppose that  $\mathbf{v} = (v_1, \dots, v_r)$  is a Parshin-chain of length  $r$  on  $K$  and let  $1 \leq s \leq r$  be given. Then the restricted collection  $\mathbf{v}_{\leq s} := (v_1, \dots, v_s)$  is a Parshin-chain of length  $s$  on  $K$ . Similarly, the collection  $\mathbf{v}_{> s} := (v_{s+1}, \dots, v_r)$  is a Parshin-chain of length  $r-s$  on  $\kappa(\mathbf{v}_{\leq s}) = \kappa(v_s)$ . Moreover, we see that  $\mathbf{v}_{\leq s}^\circ$  is a coarsening of  $\mathbf{v}^\circ$ , and that  $\mathbf{v}^\circ = \mathbf{v}_{> s}^\circ \circ \mathbf{v}_{\leq s}^\circ$ .

**2.4. Discrete Parshin-chains and tame symbols.** We will say that a Parshin-chain  $\mathbf{v} = (v_1, \dots, v_r)$  on  $K$  is **discrete** provided that  $\Gamma_{v_i} = \mathbb{Z}$  for all  $i = 1, \dots, r$ . Given  $x_1, \dots, x_r \in K$ , we say that  $\mathbf{x} = (x_1, \dots, x_r)$  is a **uniformizing system** for a discrete Parshin-chain  $\mathbf{v} = (v_1, \dots, v_r)$  on  $K$  if  $x_1, \dots, x_r \in K$  satisfy the following (inductive) conditions:

- (1) If  $r = 1$ , then  $\mathbf{x} = (x_1)$  is a uniformizing system for  $\mathbf{v} = (v_1)$  if and only if  $v_1(x_1) = 1$ . I.e. a uniformizing system for a discrete valuation  $v$ , considered as a length-1 Parshin-chain, is simply a uniformizer for  $v$ .
- (2) If  $r > 1$ , suppose uniformizing systems have been defined for discrete Parshin-chains of length  $r-1$ . Then  $\mathbf{x} = (x_1, \dots, x_r)$  is a uniformizing system for  $\mathbf{v} = (v_1, \dots, v_r)$  provided that the following conditions hold:
  - (a)  $x_1$  is a uniformizer for  $v_1$ .
  - (b)  $x_2, \dots, x_r \in U_{v_1}$ .
  - (c)  $(\bar{x}_2, \dots, \bar{x}_r)$  is a uniformizing system for  $(v_2, \dots, v_r)$ , where  $\bar{x}_i$  denotes the image of  $x_i$  in  $\kappa(v_1)$ .

It is easy to see that uniformizing systems always exist for any discrete Parshin-chain  $\mathbf{v} = (v_1, \dots, v_r)$  of any length. Moreover, if  $\mathbf{x} = (x_1, \dots, x_r)$  is a uniformizing system for  $\mathbf{v} = (v_1, \dots, v_r)$ , and  $1 \leq s \leq r$ , then  $(x_1, \dots, x_s)$  is a uniformizing system for  $\mathbf{v}_{\leq s} = (v_1, \dots, v_s)$ , and  $(\bar{x}_{s+1}, \dots, \bar{x}_r)$  is a uniformizing system for  $\mathbf{v}_{> s} = (v_{s+1}, \dots, v_r)$ , where  $\bar{x}_i$  denotes the image of  $x_i$  in  $\kappa(\mathbf{v}_{\leq s}) = \kappa(v_s)$ .

For a discrete Parshin-chain  $\mathbf{v} = (v_1, \dots, v_r)$ , we may compose the tame symbols associated to each  $v_i$  and obtain the **Tame symbol associated to  $\mathbf{v}$** :

$$\{\bullet\}_{\mathbf{v}} := \{\cdots \{\{\bullet\}_{v_1}\}_{v_2} \cdots\}_{v_r} : K_{*+r}^M(K) \rightarrow K_*^M(K\mathbf{v}).$$

Similarly, we obtain induced homomorphisms on mod- $\ell$  Milnor K-groups  $\{\bullet\}_{\mathbf{v}} : K_{*+r}^M(K) \rightarrow k_*^M(K\mathbf{v})$ .

**2.5. Prolongations of Parshin-chains.** Suppose that  $K \hookrightarrow L$  is an extension of fields and  $\mathbf{v} = (v_1, \dots, v_r)$  is a Parshin-chain on  $K$ . We say that a Parshin-chain  $\mathbf{w}$  on  $L$  is a **prolongation** of  $\mathbf{v}$  provided that the following (inductive) conditions hold:

- (1) The length of  $\mathbf{v}$  is the same as the length of  $\mathbf{w}$ ; say both have length  $r$ , and write  $\mathbf{v} = (v_1, \dots, v_r)$  and  $\mathbf{w} = (w_1, \dots, w_r)$ .
- (2) If  $r = 1$ , then  $\mathbf{w} = (w_1)$  is a prolongation of  $\mathbf{v} = (v_1)$  if and only if the valuation  $w_1$  is a prolongation of  $v_1$  to  $L$ .
- (3) If  $r > 1$ , suppose prolongations have been defined for Parshin-chains of length  $r - 1$ . Then  $\mathbf{w} = (w_1, \dots, w_r)$  is a prolongation of  $\mathbf{v} = (v_1, \dots, v_r)$  to  $L$  provided that the following conditions hold:
  - (a)  $w_1$  is a prolongation of  $v_1$  to  $L$ . In particular this implies that  $Lw_1$  is a field extension of  $Kv_1$ .
  - (b)  $(w_2, \dots, w_r)$  is a prolongation of  $(v_2, \dots, v_r)$  to  $Lw_1$ .

Since valuations can be prolonged to any field extension, the same is true for Parshin-chains.

Suppose that  $\mathbf{v} = (v_1, \dots, v_r)$  is a *discrete* Parshin-chain on  $K$  and that  $L|K$  is a finite extension. Let  $\mathbf{w} = (w_1, \dots, w_r)$  be a prolongation of  $\mathbf{v}$  to  $L$ . It is easy to see in this case that  $\mathbf{w}$  must be a discrete Parshin-chain on  $L$ . In this context, the **ramification indices** of  $\mathbf{w}|\mathbf{v}$ , denoted  $e(\mathbf{w}|\mathbf{v}) = (e_1, \dots, e_r)$ , is a sequence of positive integers where  $e_i = e(w_i|v_i)$  is the usual ramification index of  $w_i|v_i$ .

**Lemma 2.2.** *Let  $K$  be a field and let  $\mathbf{v} = (v_1, \dots, v_r)$  be a discrete Parshin-chain on  $K$ . Let  $L|K$  be a (possibly trivial) finite extension and let  $\mathbf{w} = (w_1, \dots, w_r)$  be a prolongation of  $\mathbf{v}$  to  $L$  with ramification indices  $e(\mathbf{w}|\mathbf{v}) = (e_1, \dots, e_r)$ . Let  $(x_1, \dots, x_r)$  be a uniformizing system for  $\mathbf{v}$ . Then the following hold:*

- (1) *The following equality holds in  $K_0^M(L\mathbf{w}) = \mathbb{Z}$ :*

$$\{x_1, \dots, x_r\}_{\mathbf{w}} = e_1 \cdots e_r.$$

- (2) *Let  $y_1, \dots, y_s \in U_{\mathbf{w}}$  be given. Then the following equality holds in  $K_s^M(L\mathbf{w})$ :*

$$\{x_1, \dots, x_r, y_1, \dots, y_s\}_{\mathbf{w}} = e_1 \cdots e_r \cdot \{\bar{y}_1, \dots, \bar{y}_s\}.$$

*Proof.* Both (1) and (2) follow immediately by applying Equation (2.1)  $r$  times.  $\square$

### 3. MILNOR K-THEORY OF FUNCTION FIELDS

Throughout this section,  $k$  will denote an algebraically closed field of characteristic  $\neq \ell$ . Recall that  $K$  is called a **function field** over  $k$  if  $K$  is a finitely generated field extension of  $k$ . We say that  $X$  is a  **$k$ -variety** if  $X$  is an integral separated scheme of finite type over  $k$ .

For a (scheme-theoretic) point  $P$  in an integral  $k$ -scheme  $X$ , we denote by  $\bar{P}$  the closure of  $\{P\}$  in  $X$ , considered as a reduced (hence integral) closed subscheme of  $X$ . Also, we write  $(\mathcal{O}_{X,P}, \mathfrak{m}_P)$  for the local ring at the point  $P$ , and recall that  $k(P) = \mathcal{O}_{X,P}/\mathfrak{m}_P$  is the



function field of  $\overline{P}$ . If  $Y \rightarrow X$  is a morphism of  $k$ -schemes and  $P \in X$ , then we write  $Y_P := \operatorname{Spec} k(P) \times_X Y$  for the fiber of  $Y \rightarrow X$  over  $P$ . Finally, we note that if  $X$  is a  $k$ -variety and  $P \in X$ , then  $\overline{P}$  is a  $k$ -variety as well.

Although we will usually work with  $k$ -varieties, the following slightly more general notion of a *model* of a function field will be useful for certain definitions/constructions. If  $K|k$  is a function field, we say that  $X$  is a **model** for  $K|k$  if  $X$  is one of the following types of  $k$ -schemes:

- (1)  $X$  is a  $k$ -variety whose function field is  $K$ .
- (2)  $X = \operatorname{Spec} \mathcal{O}_{Y,y}$  for some  $k$ -variety  $Y$  whose function field is  $K$  and some  $y \in Y$ .

In particular, a model  $X$  for  $K|k$  is a  $k$ -variety if and only if  $X$  is of finite type over  $k$ .

**3.1. Prime-divisors.** Suppose that  $K$  is a function field over  $k$  and that  $X$  is a model for  $K|k$ . A regular point  $P$  of codimension 1 in  $X$  will be called a **prime-divisor** on  $X$ . Recall that a prime-divisor  $P$  on  $X$  yields a discrete valuation  $v_P$  of  $K$ , whose valuation ring is precisely  $\mathcal{O}_{X,P}$ , the local ring of  $P$  in  $X$ . We say that a valuation  $v$  of  $K$  is **divisorial** if  $v = v_P$  for some prime-divisor  $P$  on some  $k$ -variety  $Y$  such that  $k(Y) = K$ .

An  **$r$ -prime divisor** on  $X$ , denoted  $\mathbf{P} = (P_1, \dots, P_r)$ , is an ordered collection of (scheme-theoretic) points  $P_i$  of  $X$ , and is defined inductively as follows:

- (1) If  $r = 1$ , then  $\mathbf{P} = (P)$  is a 1-prime-divisor on  $X$  if and only if  $P$  is a prime-divisor on  $X$ . We will not distinguish between prime-divisors  $P$  and the associated 1-prime-divisors  $\mathbf{P} = (P)$ .
- (2) If  $r > 1$ , then  $(P_1, \dots, P_r)$  is an  $r$ -prime-divisor on  $X$  if and only if  $P_1$  is a prime-divisor on  $X$  and  $(P_2, \dots, P_r)$  is an  $(r-1)$ -prime-divisor on  $\overline{P_1}$ .

Similarly to the way in which a prime divisor yields a discrete valuation, an  $r$ -prime-divisor  $\mathbf{P} = (P_1, \dots, P_r)$  on  $X$  yields a discrete Parshin-chain of length  $r$  on  $K$ , denoted  $\mathbf{v_P}$ . Explicitly, the Parshin-chain  $\mathbf{v_P} = (v_1, \dots, v_r)$  is defined as follows:

- (1) The valuation  $v_1 = v_{P_1}$  is the valuation of  $K$  associated to  $P_1$ .
- (2) For  $i = 1, \dots, r-1$ , the valuation  $v_{i+1} = v_{P_{i+1}}$  is the valuation of  $k(P_i) = \kappa(v_i)$  associated to  $P_{i+1}$ .

In particular, if  $\mathbf{P} = (P_1, \dots, P_r)$  is an  $r$ -prime-divisor on  $X$  with associated Parshin-chain  $\mathbf{v_P} = (v_1, \dots, v_r)$ , then  $k(P_r)$ , the residue field of the scheme-theoretic point  $P_r$  in  $X$ , is precisely  $\kappa(\mathbf{v_P})$ , the residue field of the Parshin-chain  $\mathbf{v_P}$ .

**3.2. Regular parameters.** One key way to obtain an  $r$ -prime-divisor is using regular coordinates. Let  $X$  be a  $k$ -variety such that  $k(X) = K$  and let  $x$  be a *regular closed point* of  $X$ . Consider  $(A, \mathbf{m}) := (\mathcal{O}_{X,x}, \mathbf{m}_x)$  the regular local  $k$ -algebra associated to  $x \in X$ . Let  $x_1, \dots, x_d$  be a regular system of parameters for  $(A, \mathbf{m})$ . Fix  $r \leq d$  and let  $\mathbf{x} = (x_1, \dots, x_r)$ ; such an  $\mathbf{x}$  will be called a **partial system of regular parameters** of length  $r$  in  $A$ . We can associate to such a system  $\mathbf{x}$  an  $r$ -prime-divisor  $\mathbf{P_x} = (P_1, \dots, P_r)$  on  $\operatorname{Spec} A$ , by letting  $P_i$  be the generic point of  $V(x_1, \dots, x_i)$  for each  $i = 1, \dots, r$ . Since  $P_i$  is a regular point of codimension 1 in  $\operatorname{Spec} A/(x_1, \dots, x_{i-1}) = V(x_1, \dots, x_{i-1})$  for each  $i = 1, \dots, r$ , we see that  $\mathbf{P_x}$  is indeed an  $r$ -prime-divisor on  $\operatorname{Spec} A$ .

Moreover, because we started with a regular closed point  $x$  in  $X$ , it is easy to see that this construction also yields an  $r$ -prime-divisor on  $X$ , by mapping the terms of  $\mathbf{P_x}$  via the canonical map  $\operatorname{Spec} A \rightarrow X$ . We will abuse the notation and also denote by  $\mathbf{P_x}$  the associated

$r$ -prime-divisor on  $X$ . Furthermore, it is clear from the definitions that, setting  $\mathbf{P} = \mathbf{P}_{\mathbf{x}}$ , the system  $\mathbf{x}$  is a *uniformizing system* for the associated Parshin-chain  $\mathbf{v}_{\mathbf{P}}$ , as defined in §2.4.

**3.3. Prolongations of  $r$ -prime-divisors.** Suppose that  $X$  is a normal  $k$ -variety with function field  $K$ . Let  $L$  be a finite extension of  $K$  and let  $Y$  denote the normalization of  $X$  in  $L$ . Suppose that  $\mathbf{P} = (P_1, \dots, P_r)$  is an  $r$ -prime-divisor on  $X$ . We say that an  $r$ -prime-divisor  $\mathbf{Q} := (Q_1, \dots, Q_r)$  on  $Y$  is a **prolongation** of  $\mathbf{P}$  to  $L$  (or to  $Y$ ) provided that, for all  $i = 1, \dots, r$ , the map  $Y \rightarrow X$  sends  $Q_i$  to  $P_i$ . If  $\mathbf{Q}$  is a prolongation of  $\mathbf{P}$ , then the corresponding Parshin-chain  $\mathbf{v}_{\mathbf{Q}}$  is a prolongation of  $\mathbf{v}_{\mathbf{P}}$  to  $L$  as defined in §2.3.

The existence of prolongations of  $r$ -prime-divisors is a slightly delicate matter, which we describe in the next lemma.

**Lemma 3.1.** *Let  $X$  be a normal  $k$ -variety with function field  $K$ . Let  $L$  be a finite extension of  $K$  and let  $Y$  denote the normalization of  $X$  in  $L$ . Let  $\mathbf{P}$  be an  $r$ -prime-divisor on  $X$ . Then the following hold:*

- (1) *Suppose  $r = 1$  and write  $\mathbf{P} = (P)$ . Then for any  $Q \in Y_P$ , the point  $Q$  is a prime-divisor on  $Y$  which is a prolongation of  $P$ .*
- (2) *Suppose  $r > 1$  and write  $\mathbf{P} = (P_1, \dots, P_r)$ . Let  $\mathbf{Q}' = (Q_1, \dots, Q_{r-1})$  be an  $(r-1)$ -prime-divisor on  $Y$  which prolongs  $\mathbf{P}' = (P_1, \dots, P_{r-1})$ , and consider the finite cover  $\overline{Q_{r-1}} \rightarrow \overline{P_{r-1}}$  induced by  $Y \rightarrow X$ . Then for all but finitely many prime-divisors  $P_r$  of  $\overline{P_{r-1}}$ , any choice of  $Q_r \in (\overline{Q_{r-1}})_{P_r}$  yields an  $r$ -prime-divisor  $\mathbf{Q} = (Q_1, \dots, Q_r)$  which is a prolongation of  $\mathbf{P}$ .*

*Proof.* *Proof of (1):* Since  $Y \rightarrow X$  is a finite cover of normal  $k$ -varieties, the fiber  $Y_P$  is finite and consists solely of points of codimension one in  $Y$ . Each such point in  $Y_P$  is regular since  $Y$  is normal. Thus, every point  $Q \in Y_P$  is a prime divisor on  $Y$  and  $\mathbf{Q} = (Q)$  is a prolongation of  $\mathbf{P}$  by definition.

*Proof of (2):* The induced map  $\overline{Q_{r-1}} \rightarrow \overline{P_{r-1}}$  is a finite cover of (possibly non-normal)  $k$ -varieties. Thus, there exists a non-empty open subset  $U$  of  $\overline{P_{r-1}}$  such that  $U$  is contained in the regular locus of  $\overline{P_{r-1}}$ , and the preimage of  $U$  in  $\overline{Q_{r-1}}$ , say  $U'$ , is contained in the regular locus of  $\overline{Q_{r-1}}$ . Note that  $U$  contains all but finitely many of the codimension one points of  $\overline{P_{r-1}}$ .

Let  $P_r \in U$  be any such codimension one point; since  $P_r$  is regular, we note that  $\mathbf{P} = (P_1, \dots, P_r)$  is an  $r$ -prime-divisor on  $X$ . Moreover, for all  $Q_r \in (\overline{Q_{r-1}})_{P_r} \subset U'$ , the point  $Q_r$  is regular and codimension one in  $\overline{Q_{r-1}}$ . Thus  $\mathbf{Q} = (Q_1, \dots, Q_r)$  is an  $r$ -prime-divisor on  $Y$  which is a prolongation of  $\mathbf{P}$ .  $\square$

**3.4.  $\ell$ -unramified prime-divisors.** Suppose that  $(K, v) \hookrightarrow (L, w)$  is an extension of *discretely* valued fields. We say that  $w|v$  is  **$\ell$ -unramified** provided that the ramification index  $e(w|v)$  is not divisible by  $\ell$ . Similarly, if  $(K, v)$  is a discretely valued field and  $L$  is a finite extension of  $K$ , we say that  $v$  is  **$\ell$ -unramified** in  $L$  if  $w|v$  is  $\ell$ -unramified for all prolongations  $w$  of  $v$  to  $L$ .

We make a similar definition for discrete Parshin-chains as follows. Suppose that  $L|K$  is a finite extension and  $\mathbf{v}$  is a *discrete* Parshin-chain of  $K$ . Suppose that  $\mathbf{w}$  is a prolongation of  $\mathbf{v}$  to  $L$  and recall that  $\mathbf{w}$  is necessarily discrete. We say that  $\mathbf{w}|\mathbf{v}$  is  **$\ell$ -unramified** provided that, setting  $e(\mathbf{w}|\mathbf{v}) = (e_1, \dots, e_r)$ , the ramification index  $e_i$  is not divisible by  $\ell$  for all

$i = 1, \dots, r$ . We say that  $\mathbf{v}$  is  $\ell$ -**unramified** in  $L$  if  $\mathbf{w}|\mathbf{v}$  is  $\ell$ -unramified for all prolongations  $\mathbf{w}$  of  $\mathbf{v}$  to  $L$ .

Suppose now that  $K|k$  is a function field and that  $X$  a model for  $K$ . Let  $L$  be a finite extension of  $K$ . We say that a prime-divisor  $P$  resp.  $r$ -prime-divisor  $\mathbf{P}$  on  $X$  is  $\ell$ -**unramified** in  $L$  provided that the associated valuation  $v_P$  resp. the associated Parshin-chain  $\mathbf{v}_{\mathbf{P}}$  is  $\ell$ -unramified in  $L$ . The following Lemma shows that there are many  $\ell$ -unramified  $r$ -prime-divisors on a  $k$ -variety.

**Lemma 3.2.** *Let  $k$  be an algebraically closed field of characteristic  $\neq \ell$ . Let  $X$  be a  $k$ -variety with function field  $K$  and let  $L$  be a finite extension of  $K$ . Then the following hold:*

- (1) *All but finitely many prime-divisors  $P$  on  $X$  are  $\ell$ -unramified in  $L$ .*
- (2) *Suppose that  $\mathbf{P}' = (P_1, \dots, P_{r-1})$  is an  $(r-1)$ -prime-divisor on  $X$  which is  $\ell$ -unramified in  $L$ . Then for all but finitely many prime-divisors  $P_r$  of  $\overline{P_{r-1}}$ , the  $r$ -prime-divisor  $\mathbf{P} = (P_1, \dots, P_r)$  is also  $\ell$ -unramified in  $L$ .*

*Proof.* *Proof of (1):* Let  $L^s$  be the maximal separable subextension of  $L|K$  so that  $L^s|K$  is separable and  $L|L^s$  is purely inseparable. Since  $L^s|K$  is separable, all but finitely many prime-divisors of  $X$  are *unramified* in  $L^s$ .

On the other hand, since  $L|L^s$  is purely inseparable, for all extensions of discrete valuations  $w|v$  of  $L|L^s$ , one has  $e(w|v) = p^i$  where  $p = \text{char } k \neq \ell$  and  $i$  is some non-negative integer. By the multiplicativity of ramification indices in towers of fields, we see that a prime-divisor  $P$  of  $X$  is  $\ell$ -unramified in  $L^s$  if and only if  $P$  is  $\ell$ -unramified in  $L$ . Assertion (1) of the lemma follows.

*Proof of (2):* If  $\mathbf{w}' = (w_1, \dots, w_{r-1})$  is a prolongation of  $\mathbf{v}_{\mathbf{P}'}$  to  $L$ , then assertion (1) implies that all but finitely many prime-divisors  $P_r$  on  $\overline{P_{r-1}}$  are  $\ell$ -unramified in  $\kappa(w_{r-1}) = \kappa(\mathbf{w}')$ . Since there are only finitely many prolongations  $\mathbf{w}'$  of  $\mathbf{v}_{\mathbf{P}'}$  to  $L$ , assertion (2) follows.  $\square$

### 3.5. Vanishing/non-vanishing in Milnor K-rings of function fields.

**Lemma 3.3.** *Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$  and let  $d := \text{tr.deg}(K|k)$ . Then for all  $s > d$ , one has  $k_s^M(K) = 0$ .*

*Proof.* It is well-known that the  $\ell$ -cohomological dimension of  $K$  is  $d$  (cf. [Ser02] §4.2 Proposition 11). The lemma now follows from the Bloch-Kato conjecture, which is now a theorem of VEOVODSKY-ROST et al. [Voe11], [Ros98], [Wei09].  $\square$

**Remark 3.4.** It seems that the full force of the Voevodsky-Rost Theorem is not strictly required to prove Lemma 3.3, as it suffices to prove that  $k_{r+1}^M(K) = 0$ . However, the author is not aware of a proof of Lemma 3.3 which doesn't rely on the Voevodsky-Rost Theorem.

**Lemma 3.5.** *Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ . Let  $t_1, \dots, t_r$  be given elements of  $K$  which are algebraically independent over  $k$ . Then there exist  $a_1, \dots, a_r \in k$  such that  $\{t_1 - a_1, \dots, t_r - a_r\} \neq 0$  in  $k_r^M(K)$ .*

*In particular, if  $F_1, \dots, F_r$  are subextensions of  $K|k$  such that  $\text{tr.deg}(F_i|k) = 1$  for all  $i = 1, \dots, r$  and, denoting the compositum  $F_1 \cdots F_r$  by  $F$ , one has  $\text{tr.deg}(F|k) = r$ , then there exist  $x_i \in F_i$  for  $i = 1, \dots, r$  such that  $\{x_1, \dots, x_r\} \neq 0$  in  $k_r^M(K)$ .*

*Proof.* By extending  $t_1, \dots, t_r$  to a transcendence base  $\mathbf{t} = (t_1, \dots, t_d)$  for  $K|k$ , we may assume without loss of generality that  $r = d := \text{tr.deg}(K|k)$ . Consider  $X := \mathbb{A}_{k, \mathbf{t}}^d =$

$\text{Spec } k[t_1, \dots, t_d]$ , affine  $d$ -space over  $k$  with parameters  $\mathbf{t}$ . Furthermore, consider the normalization  $Y \rightarrow X$  of  $X$  in the field extension  $k(\mathbf{t}) \hookrightarrow K$ . In particular,  $Y$  is a  $k$ -variety which is a normal model for  $K|k$ , and the map  $Y \rightarrow X$  is finite and surjective.

For a closed point  $x$  of  $X = \mathbb{A}_{k, \mathbf{t}}^d$ , say corresponding to the  $k$ -rational point  $(a_1, \dots, a_d) \in \mathbb{A}_{k, \mathbf{t}}^d(k)$ , consider the system of regular parameters  $\mathbf{x}(x) = (t_1 - a_1, \dots, t_d - a_d)$  at  $x$ , as well as the corresponding  $d$ -prime divisor  $\mathbf{P}_x := \mathbf{P}_{\mathbf{x}(x)}$  on  $X$  (cf. §3.2). By Lemma 3.2, there exists a closed point  $x_0$  in  $X$  such that  $\mathbf{P}_{x_0}$  is  $\ell$ -unramified in the finite extension  $K|k(\mathbf{t})$ . For the rest of the proof, we will denote  $\mathbf{P}_{x_0}$  by  $\mathbf{P}$  and  $\mathbf{x}(x_0)$  by  $\mathbf{x}$  for such an  $x_0$ .

Let  $\mathbf{w}$  be a prolongation of  $\mathbf{v} := \mathbf{v}_{\mathbf{P}}$  to  $K$  and consider  $e(\mathbf{w}|\mathbf{v}) = (e_1, \dots, e_d)$ . Recall that  $\mathbf{x} = (t_1 - a_1, \dots, t_d - a_d)$  is a uniformizing system for  $\mathbf{v}$ , and that,  $\mathbf{v}$  being  $\ell$ -unramified in  $K$ , the ramification index  $e_i$  is not divisible by  $\ell$  for all  $i = 1, \dots, d$ . Moreover, by Lemma 2.2, we see that  $\{t_1 - a_1, \dots, t_d - a_d\}_{\mathbf{w}} = e_1 \cdots e_d$  in  $\mathbb{Z} = K_0^M(K\mathbf{w})$ . Since  $\ell$  doesn't divide  $e_1 \cdots e_d$ , we deduce that  $\{t_1 - a_1, \dots, t_d - a_d\}_{\mathbf{w}} \neq 0$  in  $\mathbb{Z}/\ell = k_0^M(K\mathbf{w})$ . In particular,  $\{t_1 - a_1, \dots, t_d - a_d\} \neq 0$  in  $k_d^M(K)$ , and this completes the proof of the lemma.  $\square$

The following proposition is needed to relate transcendence degree to the mod- $\ell$  Milnor dimension of relatively algebraically closed subextensions of  $K|k$ . This will play a key role in §5. For a related result/argument, see POP [Pop12b] Proposition 40(3).

**Proposition 3.6.** *Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ , and let  $d := \text{tr. deg}(K|k)$ . Let  $L$  be a relatively algebraically closed subextension of  $K|k$  such that  $r := \text{tr. deg}(L|k) < d$ . Let  $z \in K^\times \setminus L^\times \cdot K^{\times \ell}$  be given. Then there exist  $x_1, \dots, x_r \in L^\times$  such that  $\{x_1, \dots, x_r, z\} \neq 0$  in  $k_{r+1}^M(K)$ .*

*Proof.* Let  $A$  be a regular  $k$ -algebra of finite type over  $k$ , whose fraction field is  $L$ ; thus  $S := \text{Spec } A$  is an affine regular  $k$ -variety which is a model for  $L|k$ . Choose a transcendence base  $\mathbf{t} = (t_1, \dots, t_s)$  for  $K|L$ , and let  $K_0 = L(\mathbf{t})$ . Thus,  $K|K_0$  is a finite extension, although it is not necessarily separable. Let  $K_1$  denote the maximal separable subextension of  $K|K_0$  so that  $K|K_1$  is purely inseparable. Since  $k_1^M(K_1) \rightarrow k_1^M(K)$  is an isomorphism (Fact 2.1), we may assume without loss of generality that  $z \in K_1$ . We let  $K_2 = K_1[\sqrt[\ell]{z}]$  and note that  $K_2|K_1$  is  $\mathbb{Z}/\ell$ -Galois and that  $K_2|K_0$  is separable. Since  $L$  is algebraically closed in  $K_1$ , the assumption that  $z \notin L^\times \cdot K^{\times \ell}$  ensures that  $L$  is also algebraically closed in  $K_2$ ; hence  $K_2|L$  is a regular extension.

Let  $B_0 = A[\mathbf{t}]$  be the polynomial algebra over  $A$  in the variables  $\mathbf{t}$ . We denote by  $B_i$  the normalization of  $B_0$  in  $K_i$  for  $i = 1, 2$ , and we denote  $\text{Spec } B_i$  by  $X_i$  for  $i = 0, 1, 2$ . Thus we have canonical maps  $X_2 \rightarrow X_1 \rightarrow X_0 \rightarrow S = \text{Spec } A$ , with  $k(X_i) = K_i$ , and  $X_i$  normal in its function field. For each  $i = 0, 1, 2$ , the extension  $K_i|L$  is regular, and therefore the fibers of  $X_i \rightarrow S$  are generically geometrically integral. Thus, we may replace  $S$  with an affine open (i.e. replacing  $A$  by a localization of the form  $A[1/f]$  for some non-zero  $f \in A$ ) and assume without loss of generality that  $(X_i)_s$ , the fiber of  $X_i \rightarrow S$  over  $s \in S$ , is integral for all  $s \in S$  and for each  $i = 0, 1, 2$ . In particular,  $(X_1)_s$  is irreducible and we will let  $\eta_s \in X_1$  denote the generic point of  $(X_1)_s$  for any  $s \in S$ .

Recall that  $K_2 = K_1[\sqrt[\ell]{z}]$ , and that  $B_2$  is the normalization of  $B_1$  in  $K_2$ . Thus, there exists some non-zero  $f_0 \in B_1$  such that  $z \in B_1[1/f_0]$  and  $B_2[1/f_0] = B_1[1/f_0, \sqrt[\ell]{z}]$ . By replacing  $S$  with an affine open, we may further assume without loss of generality that for all points  $s$  of  $S$ , the fiber  $(X_1)_s$  of  $X_1 \rightarrow S$  is not contained in  $V(f_0)$ , the zero-locus of this  $f_0$ . This

implies that for all  $s \in S$ , one has  $z \in \mathcal{O}_{X_1, \eta_s}$ , and  $k((X_2)_s) = k((X_1)_s)[\sqrt[\ell]{\bar{z}}]$ , where  $\bar{z}$  denotes the image of  $z$  under the canonical map  $\mathcal{O}_{X_1, \eta_s} \rightarrow k(\eta_s) = k((X_1)_s)$ .

Since  $K_2|L$  is a regular extension, by the Bertini-Noether theorem (cf. [FJ08] Proposition 9.4.3), we can replace  $S$  by an affine open and assume without loss of generality that for all closed points  $s$  of  $S$ , one has  $[k((X_2)_s) : k((X_0)_s)] = [K_2 : K_0]$ . In particular, this implies that for all closed points  $s$  of  $S$ , one has  $[k((X_2)_s) : k((X_1)_s)] = [K_2 : K_1] = \ell$ . By the discussion above, we deduce that for all closed points  $s$  of  $S$ , the image  $\bar{z}$  of  $z$  in  $k((X_1)_s)^\times$  is not an  $\ell$ -th power in  $k((X_1)_s)^\times$ . In particular, note that this implies  $z \in \mathcal{O}_{X_1, \eta_s}^\times$  for all closed points  $s \in S$ .

Now let  $s$  be a closed point of  $S$  and let  $x_1, \dots, x_r$  be a regular system of parameters for  $s$ . Then  $\mathbf{x} = (x_1, \dots, x_r)$  is a *partial system of regular parameters* of some closed point on  $X_0$  which lies in  $(X_0)_s$ . Thus, we may produce the associated  $r$ -prime divisor  $\mathbf{P}_{\mathbf{x}}$  on  $X_0$  (cf. §3.2), as well as the associated discrete Parshin-chain  $\mathbf{v} := \mathbf{v}_{\mathbf{P}_{\mathbf{x}}}$  on  $K_0 = L(\mathbf{t})$ . We see from the construction that  $\kappa(\mathbf{v}_{\mathbf{x}})$  is precisely  $k((X_0)_s)$ . Using Lemmas 3.1 and 3.2, it is clear that we can choose the regular closed point  $s$  of  $S$  and the regular system of parameters  $\mathbf{x}$  for  $s$  in such a way so that the following two conditions hold:

- (1) The Parshin-chain  $\mathbf{v}_{\mathbf{P}_{\mathbf{x}}} = \mathbf{v}$  is  $\ell$ -unramified in  $K_1$ .
- (2) The  $r$ -prime divisor  $\mathbf{P}_{\mathbf{x}}$  on  $X_0$  has a prolongation  $\mathbf{Q} = (Q_1, \dots, Q_r)$  which is an  $r$ -prime divisor on  $X_1$  such that  $Q_r = \eta_s$  is the generic point of  $(X_1)_s$ .

Setting  $\mathbf{w} := v_{\mathbf{Q}}$ , the discrete Parshin-chain associated to  $\mathbf{Q}$  as in (2) above, we see that  $\mathbf{w}$  is a prolongation of  $\mathbf{v}$  to  $K_1$ , and that  $\kappa(\mathbf{w}) = k((X_1)_s)$ . Furthermore, we have  $z \in U_{\mathbf{w}}$  since  $z \in \mathcal{O}_{X_1, \eta_s}^\times$ .

Now let  $\mathbf{x} = (x_1, \dots, x_r)$  and  $\mathbf{w}|\mathbf{v}$  be as above. Setting  $e(\mathbf{w}|\mathbf{v}) = (e_1, \dots, e_r)$ , we recall that for all  $i = 1, \dots, r$ , the ramification index  $e_i$  is not divisible by  $\ell$ , since  $\mathbf{v}$  is  $\ell$ -unramified in  $K_1$ . By Lemma 2.2, we see that

$$\{x_1, \dots, x_r, z\}_{\mathbf{w}} = e_1 \cdots e_r \cdot \bar{z} \in K_1^M(\kappa(\mathbf{w})) = K_1^M(k((X_1)_s)).$$

But  $e_1 \cdots e_r$  is not divisible by  $\ell$ , and recall that  $\bar{z}$  is not an  $\ell$ -th power in  $\kappa(\mathbf{w})^\times = k((X_1)_s)^\times$ . In particular,  $\{x_1, \dots, x_r, z\}_{\mathbf{w}}$  is non-trivial as an element of  $k_1^M(\kappa(\mathbf{w}))$ . We deduce that  $\{x_1, \dots, x_r, z\} \neq 0$  in  $k_{r+1}^M(K_1)$ . Finally, since  $K|K_1$  is purely inseparable, Fact 2.1 implies that  $\{x_1, \dots, x_r, z\} \neq 0$  in  $k_{r+1}^M(K)$ . This completes the proof of the proposition.  $\square$

#### 4. GRADED LATTICES

A **graded lattice**  $\mathfrak{L}^* = \coprod_{r \geq 0} \mathfrak{L}^r$  is a partially ordered graded set which satisfies the following properties:

- (1) Every subset  $S \subset \mathfrak{L}^*$  has a least upper bound  $\vee S$  and a greatest lower bound  $\wedge S$ . Namely,  $\mathfrak{L}^*$  is a *complete* lattice.
- (2) If  $a \in \mathfrak{L}^r$  and  $b \in \mathfrak{L}^s$  are such that  $a < b$ , then  $r < s$ . Namely, the partial ordering of  $\mathfrak{L}^*$  respects the grading.

An isomorphism of graded lattices  $f^* : \mathfrak{L}_1^* \rightarrow \mathfrak{L}_2^*$  is a graded bijection  $f^* = \coprod_{i \geq 0} f^i$  on the underlying sets which respects the partial ordering. The set of isomorphisms  $\mathfrak{L}_1^* \rightarrow \mathfrak{L}_2^*$  will be denoted by  $\text{Isom}^*(\mathfrak{L}_1^*, \mathfrak{L}_2^*)$ .



**4.1. The graded lattice of algebraic closure.** Let  $K|k$  be an arbitrary extension of fields of finite transcendence degree and assume that  $k$  is algebraically closed in  $K$ . We define a graded lattice  $\mathbb{G}^*(K|k) = \coprod_{r \geq 0} \mathbb{G}^r(K|k)$ , as follows:

- (1)  $\mathbb{G}^r(K|k) := \{\overline{k(t_1, \dots, t_r)} \cap K : t_1, \dots, t_r \in K, \text{tr.deg}(k(t_1, \dots, t_r)|k) = r\}$ .
- (2) The partial ordering on  $\mathbb{G}^*(K|k)$  is induced by inclusion of subextensions of  $K|k$ .

Namely,  $\mathbb{G}^*(K|k)$  is the partially ordered set of all relatively algebraically closed subextensions of  $K|k$ , while the graded component  $\mathbb{G}^r(K|k)$  consists of the relatively algebraically closed subextensions of  $K|k$  which have transcendence degree  $r$  over  $k$ .

For a subset  $S \subset \mathbb{G}^*(K|k)$ , define  $k(S)$  to be the compositum of the elements of  $S$  as subfields of  $K$ , and let  $\kappa_S := \overline{k(S)} \cap K$  be the algebraic closure of  $k(S)$  in  $K$ . We immediately see that  $\kappa_S$  is an element of  $\mathbb{G}^*(K|k)$ , and that  $\kappa_S = \vee S$  is the least upper bound of  $S$ . The greatest lower bound  $\wedge S$  of  $S$  is simply  $\cap S$ , the intersection of the elements of  $S$  considered as subfields of  $K$  which contain  $k$ .

**4.2. The map  $\Omega_K$  and algebraic closure mod- $\ell$ .** Let  $K|k$  be an arbitrary extension of fields of finite transcendence degree and assume that  $k$  is algebraically closed in  $K$ . For a subset  $S$  of  $K$ , we define  $\Omega_K(S)$  to be the *image* of the composition:

$$S \cap K^\times \hookrightarrow K^\times \twoheadrightarrow K^\times / \ell = k_1^M(K).$$

Thus,  $\Omega_K(S)$  is always a subset of  $k_1^M(K)$ , and  $\Omega_K$  is *weakly monotone*:  $S \subsetneq T \subset K$  implies  $\Omega_K(S) \subset \Omega_K(T)$ .

For a given  $r \geq 0$ , define

$$\mathfrak{G}^r(K|k) := \{\Omega_K(L) : L \in \mathbb{G}^r(K|k)\}.$$

Thus, each  $\mathfrak{G}^r(K|k)$  is a collection of subgroups of  $k_1^M(K)$ . We furthermore define

$$\mathfrak{G}^*(K|k) := \bigcup_{r \geq 0} \mathfrak{G}^r(K|k)$$

with the union being taken inside the power-set of  $k_1^M(K)$ . Namely,  $\mathfrak{G}^*(K|k)$  is also a collection of subgroups of  $k_1^M(K)$ , *without repetition*. We consider  $\mathfrak{G}^*(K|k)$  as a partially ordered set where the ordering is given by inclusion of subgroups of  $k_1^M(K)$ .

However, note that  $\mathfrak{G}^*(K|k)$  need not be a graded set whose graded components are  $\mathfrak{G}^r(K|k)$ . Namely, if there exist  $L_1 \in \mathbb{G}^r(K|k)$  and  $L_2 \in \mathbb{G}^s(K|k)$  with  $r \neq s$  such that  $\Omega_K(L_1) = \Omega_K(L_2)$ , then  $\mathfrak{G}^r(K|k)$  and  $\mathfrak{G}^s(K|k)$  will have a non-trivial intersection. Nevertheless,  $\Omega_K$  is a surjective map  $\mathbb{G}^*(K|k) \rightarrow \mathfrak{G}^*(K|k)$  which (weakly) preserves the ordering: if  $L_1, L_2 \in \mathbb{G}^*(K|k)$  with  $L_1 < L_2$  in the ordering of  $\mathbb{G}^*(K|k)$ , then  $\Omega_K(L_1) \leq \Omega_K(L_2)$  in the ordering of  $\mathfrak{G}^*(K|k)$ .

**4.3. Function fields.** The following proposition shows that  $\mathfrak{G}^*(K|k)$  is actually a graded lattice which is isomorphic to  $\mathbb{G}^*(K|k)$  in the special case where  $K$  is a function field over an algebraically closed field  $k$  of characteristic  $\neq \ell$ .

**Proposition 4.1.** *Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ . Then the following hold:*

- (1) *Suppose that  $L_1, L_2 \in \mathbb{G}^*(K|k)$  are given. Then  $L_1 = L_2$  if and only if  $\Omega_K(L_1) = \Omega_K(L_2)$ . In particular, if  $r \neq s$  then  $\mathfrak{G}^r(K|k)$  and  $\mathfrak{G}^s(K|k)$  are disjoint subsets of  $\mathfrak{G}^*(K|k)$ , and thus  $\mathfrak{G}^*(K|k) = \coprod_{r \geq 0} \mathfrak{G}^r(K|k)$  is a graded partially-ordered set.*

- (2) The graded partially ordered set  $\mathfrak{G}^*(K|k)$  is a graded lattice, and the map  $\Omega_K : \mathbb{G}^*(K|k) \rightarrow \mathfrak{G}^*(K|k)$  is an isomorphism of graded lattices.

*Proof. Proof of (1):* Say  $r$  and  $s$  are non-negative integers such that  $L_1 \in \mathbb{G}^r(K|k)$  and  $L_2 \in \mathbb{G}^s(K|k)$ , and assume that  $\Omega_K(L_1) = \Omega_K(L_2)$ . By Lemmas 3.3 and 3.5, we see that  $\dim_K^M(\Omega_K(L_1)) = r$  and  $\dim_K^M(\Omega_K(L_2)) = s$ , where  $\dim_K^M$  is as defined in §2.1. Since  $\Omega_K(L_1) = \Omega_K(L_2)$ , we deduce that  $r = s$ .

Now assume for a contradiction that  $L_1 \neq L_2$ . Since  $r = s$ , this implies that the fields  $L_1$  and  $L_2$  are incomparable as subfields of  $K$  because  $L_1$  and  $L_2$  are algebraically closed in  $K$ . In particular,  $\text{tr. deg}(L_1 L_2|k) > r$ . Thus, by Lemma 3.5, there exist  $x_1, \dots, x_r \in L_1$  and  $y \in L_2$  such that  $\{x_1, \dots, x_r, y\} \neq 0$  in  $k_{r+1}^M(K)$ . Since  $\Omega_K(L_1) = \Omega_K(L_2)$ , this implies that  $\dim_K^M(\Omega_K(L_1)) > r$ , which contradicts the fact that  $\dim_K^M(\Omega_K(L_1)) = r$ .

*Proof of (2):* By assertion (1), we know that  $\mathfrak{G}^*(K|k)$  is a graded partially ordered set whose graded components are  $\mathfrak{G}^r(K|k)$ . It's clear from the definition that  $\Omega_K : \mathbb{G}^*(K|k) \rightarrow \mathfrak{G}^*(K|k)$  is a surjective map which respects the grading, and by assertion (1) this map is also injective. Finally, it's clear from the definition that  $\Omega_K$  respects the partial ordering. Since  $\mathbb{G}^*(K|k)$  is a graded lattice, and  $\Omega_K : \mathbb{G}^*(K|k) \rightarrow \mathfrak{G}^*(K|k)$  is a bijection which respects the grading and partial ordering, we deduce that  $\mathfrak{G}^*(K|k)$  is also a graded lattice, and that  $\Omega_K$  is actually an isomorphism of graded lattices.  $\square$

## 5. RECOVERING THE MOD- $\ell$ LATTICE

Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$  and recall that  $\mathfrak{G}^*(K|k)$  is a graded lattice by Proposition 4.1. In this section we will show how to reconstruct this graded lattice using the mod- $\ell$  Milnor K-theory of  $K$  along with the collection of rational subgroups of  $k_1^M(K)$ . We begin by recalling the definition of *general elements* (terminology due to POP [Pop12b], [Pop12a]) and *rational subgroups*.

An element  $t \in K \setminus k$  is called a **general element** of  $K$  provided that  $k(t)$  is algebraically closed in  $K$ . Note that this condition is not intrinsic to the element  $t$ , but rather it completely depends on the ambient field  $K$ . Nevertheless, if  $L$  is a subextension of  $K|k$  such that  $L$  is algebraically closed in  $K$  and  $t \in L \setminus k$ , then  $t$  is general in  $L$  if and only if  $t$  is general in  $K$ . Also, note that if  $t$  is a general element of  $K$ , then  $t^{-1}$ ,  $t + a$  and  $a \cdot t$  are also general elements of  $K$  for all  $a \in k^\times$ .

If  $M|F$  is an extension of arbitrary fields, we say that an element  $x \in M$  is **separable in  $M$  over  $F$**  if  $x \notin M^p F$  where  $p = \text{char } F$ . By convention, if  $\text{char } F = 0$ , then every  $x \in M$  is separable in  $M$  over  $F$ . If  $F$  is understood from context, we may also omit the “over  $F$ ” from the terminology. Note in particular that if  $F$  is perfect and  $\text{char } F = p > 0$ , then  $x \in M$  is separable in  $M$  (over  $F$ ) if and only if  $x \notin M^p$ . It is important to note that this terminology differs from the usual notion of a *separable element* in an algebraic extension. Nevertheless, this terminology was introduced by POP in [Pop12b], so we use it here for the sake of consistency.

In the case where  $K$  is a function field over an algebraically closed field  $k$ , we see that any general element of  $K$  is also separable in  $K$ . In fact, any non-constant element of  $K$  is a power of some element of  $K$  which is separable in  $K$ . Moreover, if  $L$  is a relatively algebraically closed subextension of  $K|k$  and  $t \in L$ , then  $t$  is separable in  $L$  if and only if  $t$  is separable in  $K$ . The existence of many general elements is guaranteed by the following

so-called *Birational Bertini Theorem*, which works in the more general situation of regular function fields over arbitrary infinite fields.

**Fact 5.1** (Birational Bertini Theorem – cf. [Lan72] Ch. VIII, pg. 213). *Let  $F$  be an arbitrary infinite field and let  $M$  be a regular finitely-generated field extension of  $F$ . Let  $x, y \in M$  be algebraically independent over  $F$  with  $x$  separable in  $M$ . Then for all but finitely many  $a \in F$ , the field  $M$  is a regular extension of  $F(ax + y)$ , and in particular  $F(ax + y)$  is algebraically closed in  $M$ .*

Going back to the situation where  $K$  is a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ , we say that  $A$  is a **rational subgroup** of  $k_1^M(K)$  provided that there exists a general element  $t$  of  $K$  such that  $A = \Omega_K(k(t))$ . The collection of rational subgroups of  $k_1^M(K)$  is denoted by  $\mathfrak{G}_{\text{rat}}^1(K|k)$ , and we note that  $\mathfrak{G}_{\text{rat}}^1(K|k)$  is a subset of  $\mathfrak{G}^1(K|k)$ , in the notation of §4.2.

**5.1. Recovering higher-dimensional subsets.** In this subsection we show how to recover  $\mathfrak{G}^r(K|k)$  for  $r \geq 2$  using  $k_*^M(K)$  and  $\mathfrak{G}_{\text{rat}}^1(K|k)$ . We first need a lemma which easily follows from Fact 5.1.

**Lemma 5.2.** *Let  $K$  be a function field over an algebraically closed field  $k$ , and let  $L$  be a subextension of  $K|k$  such that  $\text{tr. deg}(L|k) \geq 2$  and  $L$  is algebraically closed in  $K$ . Then any element of  $L^\times$  is a product of two elements of  $L$  which are general in  $K$ .*

*Proof.* First suppose that  $a \in k^\times$ . Since  $\text{tr. deg}(L|k) \geq 2$ , by Fact 5.1, there exists an element  $t \in L$  such that  $t$  is general in  $K$ . Observe that  $t^{-1} \cdot a$  is also general in  $K$  and thus  $a = t \cdot (t^{-1} \cdot a)$  is a product of two elements of  $L$  which are general in  $K$ .

Now let  $x \in L^\times \setminus k^\times$  be given. Since  $\text{tr. deg}(L|k) \geq 2$ , we may choose  $y \in L$  which is algebraically independent from  $x$  over  $k$ . Moreover, since  $L$  is relatively algebraically closed in  $K$  and since any non-constant element of  $K$  is a power of an element which is separable in  $K$ , we may assume without loss of generality that  $y$  is separable in  $K$ . By Fact 5.1, we may replace  $y$  by  $x + ay$ , for some  $a \in k^\times$ , and assume furthermore that  $y$  is general in  $K$ . Namely,  $y$  is general (hence separable) in  $K$ , and  $x, y$  are algebraically independent over  $k$ . Note that  $1/x$  or  $y/x$  must be separable since  $y$  is separable. Thus, using Fact 5.1 again, we see that there exists some  $a \in k$  such that  $(y/x) + a \cdot (1/x) = (y + a)/x$  is also general in  $K$ . On the other hand, since  $y$  is general in  $K$ , the element  $y + a$  is also general in  $K$ . Moreover, since  $(y + a)/x$  is general in  $K$ , its inverse  $x/(y + a)$  is also general in  $K$ . Thus,  $x = (x/(y + a)) \cdot (y + a)$  is a product of two elements of  $L$  which are general in  $K$ .  $\square$

**Proposition 5.3.** *Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$  and assume that  $\text{tr. deg}(K|k) \geq 2$ . Let  $A$  be a subgroup of  $k_1^M(K)$  and let  $r \geq 2$  be given. Then the following are equivalent:*

- (1) *One has  $A \in \mathfrak{G}^r(K|k)$ .*
- (2) *The subgroup  $A$  is maximal among subgroups  $B$  of  $k_1^M(K)$  which satisfy the following two conditions:*
  - (a) *There exist a subset  $S \subset \mathfrak{G}_{\text{rat}}^1(K|k)$  such that  $B = \langle T : T \in S \rangle$ .*
  - (b) *One has  $\dim_K^M(B) = r$ .*

*Proof.* (1)  $\Rightarrow$  (2): Say  $L \in \mathbb{G}^r(K|k)$  is given such that  $A = \Omega_K(L)$ . Setting  $S_A = \{T \in \mathfrak{G}_{\text{rat}}^1(K|k) : T \subset A\}$ , it follows from Lemma 5.2 that  $A = \langle T : T \in S_A \rangle$ . Thus condition (a) holds for  $A$ . Also, condition (b) holds for  $A$  by Lemmas 3.3 and 3.5.

We must now show that  $A$  is maximal with respect to conditions (a) and (b). Suppose that  $B$  also satisfies (a) and (b) and that  $A \subset B$ . Assume for a contradiction that  $A \neq B$ . Thus, by condition (a), there exists some  $T_0 \in \mathfrak{G}_{\text{rat}}^1(K|k)$  such that  $T_0 \not\subset A$  and  $T_0 \subset B$ . Let  $F_0 \in \mathbb{G}^1(K|k)$  be given such that  $\Omega_K(F_0) = T_0$ . Since  $T_0 \not\subset A$ , we see that  $F_0$  is not contained in  $L$ . Furthermore, since  $L$  is algebraically closed in  $K$ , we deduce that  $\text{tr. deg}(F_0 L|k) = r+1$ . By Lemma 3.5, we see that there exist  $x_1, \dots, x_r \in L$  and  $y \in F_0$  such that  $\{x_1, \dots, x_r, y\} \neq 0$  in  $k_{r+1}^M(K)$ . But this implies that  $\dim_K^M(B) > r$ , which contradicts condition (b). Having obtained our contradiction, we deduce that  $A$  is indeed maximal among subgroups of  $k_1^M(K)$  which satisfy conditions (a), (b).

(2)  $\Rightarrow$  (1): Suppose that  $A$  is maximal among subgroups satisfying conditions (a) and (b). Let  $S$  be a subset of  $\mathfrak{G}_{\text{rat}}^1(K|k)$  such that  $A = \langle T : T \in S \rangle$ . For each  $T \in S$ , choose a  $t_T \in K \setminus k$  which is general in  $K$  such that  $T = \Omega_K(k(t_T))$ . Also, let  $M$  be the subfield of  $K$  generated by  $k$  and all these  $t_T$  as  $T \in S$  varies. Note that  $A \subset \Omega_K(M)$  by condition (a). By Lemmas 3.3 and 3.5, we see that condition (b) implies  $\text{tr. deg}(M|k) = r$ . Thus, there exists some  $L \in \mathbb{G}^r(K|k)$  such that  $M \subset L$ , and thus  $A \subset \Omega_K(L)$ . On the other hand,  $\Omega_K(L)$  satisfies conditions (a) and (b) by the argument above. The maximality of  $A$  implies that  $A = \Omega_K(L)$  and thus  $A \in \mathfrak{G}^r(K|k)$ .  $\square$

**5.2. Recovering one-dimensional subsets.** The next proposition shows how to recover  $\mathfrak{G}^1(K|k)$  using  $\mathfrak{G}^r(K|k)$  for  $r = 2, 3$ , the ring  $k_*^M(K)$ , and  $\mathfrak{G}_{\text{rat}}^1(K|k)$ . To state this proposition, we recall from §2.1 that  $\mathfrak{M}^1(K)$  denotes the collection of subgroups  $A$  of  $k_1^M(K)$  which are maximal among subgroups  $B$  of  $k_1^M(K)$  such that  $\dim_K^M(B) = 1$ .

**Proposition 5.4.** *Let  $K$  be a function field over an algebraically closed field  $k$  such that  $\text{char } k \neq \ell$ , and assume that  $\text{tr. deg}(K|k) \geq 4$ . Let  $A$  be a subgroup of  $k_1^M(K)$ . Then the following are equivalent:*

- (1) *One has  $A \in \mathfrak{G}^1(K|k)$ .*
- (2) *One has  $A \in \mathfrak{M}^1(K)$ , and there exist some  $D \in \mathfrak{G}_{\text{rat}}^1(K|k)$ ,  $B_1, B_2, E \in \mathfrak{G}^2(K|k)$ , and  $B'_1, B'_2, C \in \mathfrak{G}^3(K|k)$  such that the following conditions hold:*
  - (a)  $B_1 \neq B_2$  and  $D \not\subset C$ .
  - (b)  $B_1 \cup B_2 \subset C$ .
  - (c)  $B_1 \cup D \subset B'_1$  and  $B_2 \cup D \subset B'_2$ .
  - (d)  $E \subset B'_1 \cap B'_2$ .
  - (e)  $A = B_1 \cap B_2$ .

*Proof.* First we show that  $\mathfrak{G}^1(K|k) \subset \mathfrak{M}^1(K)$ . Let  $A \in \mathfrak{G}^1(K|k)$  be given. By Lemma 3.3 and the non-triviality of  $A$ , it follows that  $\dim_K^M(A) = 1$ . Suppose now that  $z \in k_1^M(K) \setminus A$ . By Proposition 3.6, there exists an element  $a \in A$  such that  $\{a, z\} \neq 0$  in  $k_2^M(K)$ . In particular,  $\dim_K^M(\langle A, z \rangle) \geq 2$ . This shows that  $A$  is indeed maximal among subgroups  $B$  of  $k_1^M(K)$  such that  $\dim_K^M(B) = 1$ , and thus  $A \in \mathfrak{M}^1(K)$ .

(1)  $\Rightarrow$  (2): The argument above shows that  $A \in \mathfrak{M}^1(K)$ . We must therefore prove the existence of  $D, B_1, B_2, E, B'_1, B'_2, C$  which satisfy the other assertions of condition (2). Let  $F \in \mathbb{G}^1(K|k)$  be given such that  $A = \Omega_K(F)$ . Let  $\mathbf{t} = (t_1, \dots, t_r)$  be a transcendence base

for  $K|F$ , and note that  $r \geq 3$  since  $\text{tr.deg}(K|k) \geq 4$  by assumption. Let  $K'$  denote the maximal separable subextension of  $K|F(\mathbf{t})$ . By replacing  $t_1$  resp.  $t_2$  by elements of the form  $t_1 + at_3$  resp.  $t_2 + bt_3$  for some  $a, b \in k$ , we may assume (by Fact 5.1) that  $K'$  is a regular extension of  $M := F(t_1, t_2)$ . Let  $M_1 := F(t_1)$  and  $M_2 := F(t_2)$  and note that both  $M_1$  and  $M_2$  are algebraically closed in  $K'$ .

**Claim.** *One has  $\Omega_{K'}(F) = \Omega_{K'}(M_1) \cap \Omega_{K'}(M_2)$ .*

*Proof.* Since  $M = F(t_1, t_2)$  is rational over  $F$  and  $M_i = F(t_i)$  for  $i = 1, 2$ , it is easy to see that  $\Omega_M(F) = \Omega_M(M_1) \cap \Omega_M(M_2)$ , as follows. First, observe that we have a short exact sequence

$$0 \rightarrow k_1^M(F) \rightarrow k_1^M(M) \xrightarrow{D} \bigoplus_P \mathbb{Z}/\ell \cdot [P] \rightarrow 0,$$

where  $P$  varies over the monic irreducible polynomials in  $F[t_1, t_2]$ , and the component map  $k_1^M(M) \rightarrow \mathbb{Z}/\ell \cdot [P]$  associated to  $P$  is the reduction of the  $P$ -adic valuation modulo  $\ell$ -th powers. The images  $D(\Omega_M(M_1))$  and  $D(\Omega_M(M_2))$  clearly intersect trivially in the right-hand-side of this exact sequence. Since  $\Omega_M(F)$  is contained in  $\Omega_M(M_1) \cap \Omega_M(M_2)$ , we deduce that  $\Omega_M(F) = \Omega_M(M_1) \cap \Omega_M(M_2)$ . To deduce the original claim, recall that the map  $k_1^M(M) \rightarrow k_1^M(K')$  is injective (as  $M$  is algebraically closed in  $K'$ ). The claim follows.  $\square$

For  $i = 1, 2$ , let  $F_i$  denote the algebraic closure of  $M_i$  in  $K$  and let  $L$  denote the algebraic closure of  $M$  in  $K$ . Since  $K|K'$  is purely inseparable, we note that, for  $i = 1, 2$ , the extension  $F_i|M_i$  is also purely inseparable.

**Claim.** *One has  $\Omega_K(F_1) \cap \Omega_K(F_2) = \Omega_K(F)$ .*

*Proof.* Consider the following commutative diagram

$$\begin{array}{ccccc} k_1^M(F) & \longrightarrow & k_1^M(M_1) & & \\ \downarrow & & \downarrow & \searrow \cong & \\ k_1^M(M_2) & \longrightarrow & k_1^M(K') & & k_1^M(F_1) \\ & \searrow \cong & & \searrow \cong & \downarrow \\ & & k_1^M(F_2) & \longrightarrow & k_1^M(K) \end{array}$$

and note that the diagonal arrows are isomorphisms by Fact 2.1. By the previous claim, we see that the top-left square in this diagram is a Cartesian square. The claim now follows easily since  $\Omega_K(F)$  is the image of  $k_1^M(F) \rightarrow k_1^M(K)$  and  $\Omega_K(F_i)$  is the image of  $k_1^M(F_i) \rightarrow k_1^M(K)$  for  $i = 1, 2$ .  $\square$

We now show how to find the various subgroups of  $k_1^M(K)$  which satisfy properties (a)-(e). We let  $B_1 := \Omega_K(F_1)$ ,  $B_2 := \Omega_K(F_2)$ , and  $C := \Omega_K(L)$ . Let  $t$  be a *general* element of  $K$  which is transcendental over  $L$ ; the existence of such an element is guaranteed by Fact 5.1. Finally, let  $B'_1 := \Omega_K(\overline{F_1(t)} \cap K)$ ,  $B'_2 := \Omega_K(\overline{F_2(t)} \cap K)$ ,  $E := \Omega_K(\overline{F(t)} \cap K)$  and  $D := \Omega_K(\overline{k(t)} \cap K) = \Omega_K(k(t))$ . Property (a) follows from Proposition 4.1, since  $F_1 \neq F_2$  and since  $t$  is transcendental over  $L$ . Properties (b), (c) and (d) are trivial to check as they just follow from the corresponding inclusion of subfields of  $K$ . Lastly, property (e) is the claim above.



(2)  $\Rightarrow$  (1): Proposition 4.1 implies the following fact which we tacitly use for the rest of the proof: Given  $W_1, W_2 \in \mathbb{G}^*(K|k)$ , one has  $W_1 \subset W_2$  if and only if  $\Omega_K(W_1) \subset \Omega_K(W_2)$ .

Choose  $F_1, F_2 \in \mathbb{G}^2(K|k)$  such that  $\Omega_K(F_i) = B_i$  and  $L \in \mathbb{G}^3(K|k)$  such that  $\Omega_K(L) = C$ . Property (b) implies that  $F_1 F_2 \subset L$ . Choose  $t$  a general element of  $K$  such that  $\Omega_K(k(t)) = \Omega_K(\overline{k(t)} \cap K) = D$ . Property (a) implies that  $F_1 \neq F_2$  and that  $t$  is transcendental over  $L$ . Moreover, property (c) implies that  $\Omega_K(\overline{F_1(t)} \cap K) = B'_1$  and  $\Omega_K(\overline{F_2(t)} \cap K) = B'_2$ . Choose  $M \in \mathbb{G}^2(K|k)$  such that  $\Omega_K(M) = E$ . Then  $M \subset \overline{F_1(t)} \cap \overline{F_2(t)} \cap K$  by property (d).

Let  $F = F_1 \cap F_2$ . Since  $F_1 \neq F_2$ , we note that  $\text{tr.deg}(F|k) \leq 1$ . Moreover, since  $F_1 F_2 \subset L$  and  $t$  is transcendental over  $L$ , we see that  $\overline{F(t)} \cap K = \overline{F_1(t)} \cap \overline{F_2(t)} \cap K$ . But  $t$  is transcendental over  $F$ , and thus

$$1 \leq \text{tr.deg}(\overline{F(t)} \cap K|k) = \text{tr.deg}(F|k) + 1 \leq 2.$$

On the other hand, we have  $M \subset \overline{F_1(t)} \cap \overline{F_2(t)} \cap K = \overline{F(t)} \cap K$ . Since  $\text{tr.deg}(M|k) = 2$  and  $M$  is algebraically closed in  $K$ , we see that  $M = \overline{F(t)} \cap K$ , and thus  $\text{tr.deg}(F|k) = 1$ .

To conclude the proof, first note that  $\Omega_K(F) \subset A$  by property (e). Also, the argument at the start of the proof (using Proposition 3.6) shows that  $\Omega_K(F)$  is an element of  $\mathfrak{M}^1(K)$  since  $F \in \mathbb{G}^1(K|k)$ . By the “maximality” in the definition of  $\mathfrak{M}^1(K)$ , any two comparable elements of  $\mathfrak{M}^1(K)$  must be identical. Since  $A \in \mathfrak{M}^1(K)$  by assumption and  $\Omega_K(F) \subset A$ , we deduce that  $A = \Omega_K(F)$ , hence  $A$  is an element of  $\mathfrak{G}^1(K|k)$ .  $\square$

## 6. COMBINATORIAL GEOMETRIES

The last key step in the proof of the “Milnor variant” of the main theorem is to show how to construct the combinatorial geometry of (relative) algebraic closure, which was considered in [EH91], [EH95] and [Gis08], using our K-theoretic data. This will be accomplished via the standard construction which produces a set with a closure operation from a graded lattice. We call this construction the  **$\mathfrak{C}$ -construction**; that is, if  $\mathfrak{L}^*$  is a graded lattice, we denote by  $\mathfrak{C}(\mathfrak{L}^*)$  the associated set with closure operation. When applied to  $\mathbb{G}^*(K|k)$ , this construction produces the combinatorial geometry considered in loc.cit.

**6.1. Closure operations.** Let  $S$  be a set and let  $\mathcal{P}(S)$  denote the power set of  $S$ . A **closure operation** on  $S$  is a function  $\text{cl} : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$  such that for all subsets  $A \subset B \subset S$ , one has  $A \subset \text{cl}(A) = \text{cl}(\text{cl}(A))$  and  $\text{cl}(A) \subset \text{cl}(B)$ . If we write  $(S, \text{cl})$ , we implicitly mean that  $S$  is a set which is equipped with a closure operation  $\text{cl}$ . Also, for a finite subset  $\{a_1, \dots, a_n\} \subset S$ , we will usually write  $\text{cl}(a_1, \dots, a_n)$  instead of  $\text{cl}(\{a_1, \dots, a_n\})$ . Finally, we define an isomorphism of sets with closure operations  $f : (S_1, \text{cl}_1) \rightarrow (S_2, \text{cl}_2)$  to be a bijection of the underlying sets  $f : S_1 \rightarrow S_2$  which is compatible with closures in the sense that  $f(\text{cl}_1(A)) = \text{cl}_2(f(A))$  for all  $A \subset S_1$ . The set of isomorphisms  $(S_1, \text{cl}_1) \rightarrow (S_2, \text{cl}_2)$  will be denoted by  $\text{Isom}^{\text{cl}}(S_1, S_2)$ .

Suppose that  $\mathfrak{L}^*$  is a graded lattice. We can associate to  $\mathfrak{L}^*$  a closure operation  $\text{cl}$  on  $\mathfrak{L}^1$ , as follows. For a subset  $A \subset \mathfrak{L}^1$ , define

$$\text{cl}(A) = \{a \in \mathfrak{L}^1 : a \leq \vee A\}.$$

Since  $\vee A$  is the least upper bound of  $A$ , we see that  $A \subset \text{cl}(A)$ . This implies that  $\vee \text{cl}(A) = \vee A$  and thus  $\vee \text{cl}(\text{cl}(A)) = \vee \text{cl}(A)$ . Therefore, we deduce that  $\text{cl}(A) = \text{cl}(\text{cl}(A))$ . Furthermore, if  $A \subset B$  then  $\text{cl}(A) \subset \text{cl}(B)$  since  $\vee A \leq \vee B$ . Thus  $\text{cl}$  is indeed a closure operation on  $\mathfrak{L}^1$ . We will denote  $(\mathfrak{L}^1, \text{cl})$  by  $\mathfrak{C}(\mathfrak{L}^*)$ .

Finally, note that the construction above is compatible with isomorphisms. In particular, any isomorphism of graded lattices  $f^* : \mathfrak{L}_1^* \rightarrow \mathfrak{L}_2^*$  induces an isomorphism of sets with closure operations  $\mathfrak{C}(f^*) : \mathfrak{C}(\mathfrak{L}_1^*) \rightarrow \mathfrak{C}(\mathfrak{L}_2^*)$  where  $f^1 : \mathfrak{L}_1^1 \rightarrow \mathfrak{L}_2^1$  is the corresponding bijection on the underlying sets. Namely, we get a canonical map of isomorphism sets:

$$\mathfrak{C} : \text{Isom}^*(\mathfrak{L}_1^*, \mathfrak{L}_2^*) \rightarrow \text{Isom}^{\text{cl}}(\mathfrak{C}(\mathfrak{L}_1^*), \mathfrak{C}(\mathfrak{L}_2^*)).$$

Moreover,  $\mathfrak{C}$  is compatible with compositions of isomorphisms in the sense that, if  $f_{12}^* : \mathfrak{L}_1^* \rightarrow \mathfrak{L}_2^*$  and  $f_{23}^* : \mathfrak{L}_2^* \rightarrow \mathfrak{L}_3^*$  are isomorphisms of graded lattices, then  $\mathfrak{C}(f_{23}^* \circ f_{12}^*) = \mathfrak{C}(f_{23}^*) \circ \mathfrak{C}(f_{12}^*)$ .

Of course, one can define *morphisms* of graded lattices resp. sets with closure in natural ways so that  $\mathfrak{C}$  is actually a functor. We will not develop these details here because this will not play any role in proving the results of this paper.

**6.2. Combinatorial geometries.** Let  $(S, \text{cl})$  be a set equipped with a closure operation. We say that  $(S, \text{cl})$  is a **combinatorial geometry** if it satisfies the following additional axioms for all  $A \subset S$  and  $a, b \in S$ :

- (1) **Exchange:** If  $a \in \text{cl}(A \cup \{b\}) \setminus \text{cl}(A)$ , then  $b \in \text{cl}(A \cup \{a\})$ .
- (2) **Finite Character:** If  $a \in \text{cl}(A)$ , then  $a \in \text{cl}(B)$  for some finite subset  $B$  of  $A$ .
- (3) **Geometry:**  $\text{cl}(\emptyset) = \emptyset$  and  $\text{cl}(\{a\}) = \{a\}$ .

We will need to speak about definable sets in the first-order language of a combinatorial geometry (or, more generally, a set with closure operation). The language which we use is the standard one,  $\mathcal{L}_{\text{cl}} = (\text{cl}_n)_{n \geq 0}$ , which consists entirely of relation symbols, where  $\text{cl}_n$  is an  $(n+1)$ -ary relation. For a set with closure operation  $S = (S, \text{cl})$ , we interpret  $S$  as an  $\mathcal{L}_{\text{cl}}$ -structure as follows. The universe of a given structure is precisely the underlying set  $S$ . For each  $n$ , the  $(n+1)$ -ary relation  $\text{cl}_n(x_0; x_1, \dots, x_n)$  defines the closure  $\text{cl}(a_1, \dots, a_n)$  by saying

$$\text{cl}_n(a_0; a_1, \dots, a_n) \iff a_0 \in \text{cl}(a_1, \dots, a_n).$$

To simplify the notation, we will use underlined boldface characters to denote (possibly empty) tuples of variables and/or constants of a given length; the length of a tuple  $\underline{x}$  will be denoted by  $l(\underline{x})$ . For example, we abbreviate  $(x_1, \dots, x_r)$  as  $\underline{x}$  and set  $l(\underline{x}) = r$ . For  $\psi(\underline{x})$ , a first-order formula in  $\mathcal{L}_{\text{cl}}$  with  $l(\underline{x})$  free variables, one defines:

$$\psi(S) = \{\underline{c} \in S^{l(\underline{x})} : \psi(\underline{c}) \text{ holds true in } S\}.$$

Recall that a set  $A$  is called a  **$\emptyset$ -definable** subset of  $S^r$  if there exists some first-order  $\mathcal{L}_{\text{cl}}$ -formula, say  $\psi(\underline{x})$ , such that  $r = l(\underline{x})$  and  $A = \psi(S)$ . Similarly, for  $\psi(\underline{x}; \underline{y})$ , a first-order formula in  $\mathcal{L}_{\text{cl}}$  with  $l(\underline{x}) + l(\underline{y})$  free variables, and  $\underline{b} \in S^{l(\underline{y})}$ , one defines:

$$\psi(S; \underline{b}) = \{\underline{c} \in S^{l(\underline{x})} : \psi(\underline{c}; \underline{b}) \text{ holds true in } S\}.$$

Given a non-empty subset  $P \subset S$ , the set  $A$  is called a  **$P$ -definable** subset of  $S^r$  if there exists a some first-order  $\mathcal{L}_{\text{cl}}$ -formula, say  $\psi(\underline{x}; \underline{y})$ , and some  $\underline{b} \in P^{l(\underline{y})}$ , such that  $r = l(\underline{x})$  and  $A = \psi(S; \underline{b})$ . We say that  $A$  is **definable** if it is a  $P$ -definable subset of  $S^r$  for some  $r$  and for some (possibly empty) subset  $P$  of  $S$ . For example, if  $a_1, \dots, a_s$  are elements of  $S$ , then the closure  $\text{cl}(a_1, \dots, a_s)$  is a definable subset of  $S$  since:

$$\text{cl}(a_1, \dots, a_s) = \text{cl}_n(S; a_1, \dots, a_s).$$

Note that the *finite character* axiom for a combinatorial geometry ensures that the full structure of a combinatorial geometry  $S$ , as a set with closure operation, can be recovered from the  $\mathcal{L}_{\text{cl}}$ -structure of  $S$ .

**6.3. Combinatorial geometry of algebraic closure.** Let  $K|k$  be an extension of fields of finite transcendence degree and assume that  $k$  is algebraically closed in  $K$ . We denote  $\mathfrak{C}(\mathbb{G}^*(K|k))$  by  $\mathbb{G}(K|k)$ . In other words,  $\mathbb{G}(K|k)$  is a set with a closure operation whose underlying set is precisely  $\mathbb{G}^1(K|k)$ .

The closure operation on  $\mathbb{G}(K|k)$  can be described explicitly as follows. For  $t \in K \setminus k$ , define  $\kappa_t := \overline{k(t)} \cap K$ . Thus, the underlying set of  $\mathbb{G}(K|k)$  is precisely

$$\mathbb{G}^1(K|k) = \{\kappa_t : t \in K \setminus k\}$$

which is the collection of relatively algebraically closed subextensions of  $K|k$  of transcendence degree 1 over  $k$ . For a subset  $S \subset \mathbb{G}^1(K|k)$ , denote by  $k(S)$  the compositum of the terms in  $S$  (as subfields of  $K$ ) and denote by  $\kappa_S$  the field  $\overline{k(S)} \cap K$ , as in §4.1. The closure of  $S$  is defined as follows:

$$\text{cl}(S) = \{\kappa_t \in \mathbb{G}^1(K|k) : \kappa_t \subset \kappa_S\}.$$

It is fairly straightforward to check that  $\mathbb{G}(K|k)$  is actually a *combinatorial geometry*, and that  $\mathbb{G}(K|k)$  is precisely  $\mathfrak{C}(\mathbb{G}^*(K|k))$ , the set with closure operation associated to the graded lattice  $\mathbb{G}^*(K|k)$  via the  $\mathfrak{C}$ -construction of §6.1.

Suppose now that  $K|k$  and  $L|l$  are function fields over algebraically closed fields  $k$  resp.  $l$ . Then any isomorphism  $\sigma : K^i \rightarrow L^i$  such that  $\sigma k = l$  induces an isomorphism  $\mathbb{G}(K^i|k) \rightarrow \mathbb{G}(L^i|l)$ . Thus, we have a canonical map  $\text{Isom}^i(K, L) \rightarrow \text{Isom}^{\text{cl}}(\mathbb{G}(K^i|k), \mathbb{G}(L^i|l))$ . It is clear that this map is compatible with compositions of isomorphisms (i.e.  $\mathbb{G}$  is functorial with respect to isomorphisms).

If  $\text{char } k = p > 0$ , then the Frobenius isomorphism  $\text{Frob}_p : K^i \rightarrow K^i$  induces the *identity* isomorphism on  $\mathbb{G}(K^i|k)$ . Thus, we obtain an induced map

$$\text{Isom}_F^i(K, L) \rightarrow \text{Isom}^{\text{cl}}(\mathbb{G}(K^i|k), \mathbb{G}(L^i|l)).$$

Finally, we have a canonical isomorphism of combinatorial geometries  $\mathbb{G}(K|k) \cong \mathbb{G}(K^i|k)$  defined on underlying sets by sending  $F \in \mathbb{G}^1(K|k)$  to  $\overline{F} \cap K^i = F^i \in \mathbb{G}^1(K^i|k)$ . To summarize, we have a canonical map of isomorphism sets which is compatible with composition of isomorphisms:

$$\text{Isom}_F^i(K, L) \rightarrow \text{Isom}^{\text{cl}}(\mathbb{G}(K|k), \mathbb{G}(L|l)).$$

The main results concerning the classification of combinatorial geometries of algebraic closure were first developed for extensions of algebraically closed fields by EVANS-HRUSHOVSKI [EH91], [EH95]. These results were extended to extensions of arbitrary fields by GISMATULLIN [Gis08] using similar arguments. These main results essentially assert that  $K^i$  is encoded in  $\mathbb{G}(K|k)$  in a first-order way, independent from  $K|k$ , using the language  $\mathcal{L}_{\text{cl}}$  from §6.2. We summarize this theorem from loc.cit. in a special case which we will need in order to prove Theorem B.

**Theorem 6.1** ([Gis08] Theorem 4.2). *Let  $k, l$  be algebraically closed fields and let  $K|k$  and  $L|l$  be function fields such that  $\text{tr. deg}(K|k) \geq 5$ . Then the following hold:*

- (1) *The field  $K^i$  is uniformly interpretable (with parameters) in  $\mathbb{G}(K|k)$ .*

- (2) Any isomorphism  $\sigma : \mathbb{G}(K|k) \rightarrow \mathbb{G}(L|l)$  of combinatorial geometries is induced by an isomorphism of fields  $\tilde{\sigma} : K^i \rightarrow L^i$ , which is unique up-to Frobenius twists, such that  $\tilde{\sigma}k = l$ . Namely, the following canonical map is a bijection:

$$\text{Isom}_F^i(K, L) \rightarrow \text{Isom}^{\text{cl}}(\mathbb{G}(K|k), \mathbb{G}(L|l)).$$

We mention Theorem 6.1(1) in particular to stress that the process to reconstruct  $K^i|k$  from  $\mathcal{K}_{\text{rat}}^{\text{M}}(K|k)$  in Theorem B(1) can be made very explicit (although it is not effective due to the use of Propositions 5.3 and 5.4). In simpler terms, Theorem 6.1(1) says that there are first-order formulas  $P(\underline{\mathbf{y}})$ ,  $U(\underline{\mathbf{x}}_1; \underline{\mathbf{y}})$ ,  $E(\underline{\mathbf{x}}_2; \underline{\mathbf{y}})$ ,  $A(\underline{\mathbf{x}}_3; \underline{\mathbf{y}})$  and  $M(\underline{\mathbf{x}}_4; \underline{\mathbf{y}})$  in  $\mathcal{L}_{\text{cl}}$ , which are *independent* of  $K|k$ , such that for all  $K|k$  as in the theorem, and any *arbitrary choice* of  $\underline{\mathbf{b}} \in P(\mathbb{G}(K|k))$ , the following hold for  $\mathbb{G} := \mathbb{G}(K|k)$ :

- (1) One has  $E(\mathbb{G}; \underline{\mathbf{b}}) \subset U(\mathbb{G}; \underline{\mathbf{b}})^2$ , and this subset is an equivalence relation on  $U(\mathbb{G}; \underline{\mathbf{b}})$ . Let  $\mathbf{U}$  denote the set of equivalence classes of this equivalence relation.
- (2) There are binary operations  $+^{\mathbb{G}}$  and  $\times^{\mathbb{G}}$  on  $\mathbf{U}$  such that  $A(\mathbb{G}; \underline{\mathbf{b}})$  resp.  $M(\mathbb{G}; \underline{\mathbf{b}})$  is the preimage of the graph of  $+^{\mathbb{G}}$  resp.  $\times^{\mathbb{G}}$  under the projection  $U(\mathbb{G}, \underline{\mathbf{b}})^3 \rightarrow \mathbf{U}^3$ .
- (3) There is a bijection  $K^i \xrightarrow{\cong} \mathbf{U}$  of sets which induces an isomorphism of structures  $(K^i, +, \times) \cong (\mathbf{U}, +^{\mathbb{G}}, \times^{\mathbb{G}})$ .

In particular,  $(\mathbf{U}, +^{\mathbb{G}}, \times^{\mathbb{G}})$  is a field where the addition  $+^{\mathbb{G}}$  defined by  $A(\mathbb{G}; \underline{\mathbf{b}})$ , the multiplication  $\times^{\mathbb{G}}$  is defined by  $M(\mathbb{G}; \underline{\mathbf{b}})$ , and this field is isomorphic to  $K^i$ . Thus the field  $K^i$  can be reconstructed from  $\mathbb{G}(K|k)$  using the formulas  $P, U, E, A$  and  $M$  which are independent of  $K|k$ . The subfield  $k$  can then be recovered from  $K^i$  as the collection of (multiplicatively) divisible elements of  $K^i$ , since  $K$  is a function field over  $k = \bar{k}$ .

## 7. PROOF OF THEOREM B

We will use the notation of Theorem B. Namely,  $K|k$  and  $L|l$  are function fields over algebraically closed fields such that  $\text{char } k, \text{char } l \neq \ell$  and  $\text{tr. deg}(K|k) \geq 5$ .

*Proof of (1):* We start with our given data  $\mathcal{K}_{\text{rat}}^{\text{M}}(K|k)$ :

- The groups  $k_1^{\text{M}}(K)$  and  $k_2^{\text{M}}(K)$ .
- The multiplication map  $k_1^{\text{M}}(K) \otimes k_1^{\text{M}}(K) \rightarrow k_2^{\text{M}}(K)$ .
- The collection  $\mathfrak{G}_{\text{rat}}^1(K|k)$  of rational subgroups of  $k_1^{\text{M}}(K)$ .

The work required to reconstruct the field  $K^i|k$  from  $\mathcal{K}_{\text{rat}}^{\text{M}}(K|k)$  has already been done, and now it's just a matter of putting everything together. The following are the steps which reconstruct  $K^i|k$  from  $\mathcal{K}_{\text{rat}}^{\text{M}}(K|k)$ .

- (1) First, we can reconstruct the whole mod- $\ell$  Milnor K-ring  $k_*^{\text{M}}(K)$  using  $\mathcal{K}_{\text{rat}}^{\text{M}}(K|k)$ , since  $k_*^{\text{M}}(K)$  is a quadratic algebra. More precisely, we have:

$$k_*^{\text{M}}(K) = \frac{T_*(k_1^{\text{M}}(K))}{\langle \ker(k_1^{\text{M}}(K) \otimes k_1^{\text{M}}(K) \rightarrow k_2^{\text{M}}(K)) \rangle}$$

where  $T_*(k_1^{\text{M}}(K))$  is the (graded) tensor-algebra generated by  $k_1^{\text{M}}(K)$  in degree 1, and  $\langle \ker(k_1^{\text{M}}(K) \otimes k_1^{\text{M}}(K) \rightarrow k_2^{\text{M}}(K)) \rangle$  is the ideal of  $T_*(k_1^{\text{M}}(K))$  generated by the kernel of the multiplication map  $k_1^{\text{M}}(K) \otimes k_1^{\text{M}}(K) \rightarrow k_2^{\text{M}}(K)$ . In step (2) below, we will tacitly use the fact that we have constructed the full mod- $\ell$  Milnor K-ring  $k_*^{\text{M}}(K)$  of  $K$ . In particular, we are now able to compute the Milnor-dimensions of subsets of  $k_1^{\text{M}}(K)$ .

- (2) Recall that  $\mathfrak{G}^*(K|k)$  is a graded lattice by Proposition 4.1. Using  $k_*^M(K)$  along with the collection  $\mathfrak{G}_{\text{rat}}^1(K|k)$ , we next reconstruct this graded lattice  $\mathfrak{G}^*(K|k)$  using the following recipe:
- (a) Proposition 5.3 shows how to reconstruct  $\mathfrak{G}^r(K|k)$  for  $r \geq 2$  using  $k_*^M(K)$  and  $\mathfrak{G}_{\text{rat}}^1(K|k)$ .
  - (b) Having reconstructed  $\mathfrak{G}^r(K|k)$  for  $r \geq 2$ , Proposition 5.4 now shows how to reconstruct  $\mathfrak{G}^1(K|k)$  using  $k_*^M(K)$  and  $\mathfrak{G}_{\text{rat}}^1(K|k)$ .
  - (c) The partial ordering on  $\mathfrak{G}^*(K|k)$  arises from inclusion of subgroups in  $k_1^M(K)$ .
  - (d) The grading of  $\mathfrak{G}^*(K|k)$  is recovered as part of Propositions 5.3 and 5.4. Alternatively, Lemmas 3.3 and 3.5 provide the following recipe to recover the grading: For an element  $A \in \mathfrak{G}^*(K|k)$  one has  $\dim_K^M(A) = r$  if and only if  $A \in \mathfrak{G}^r(K|k)$ .
- (3) Since  $\mathfrak{G}^*(K|k)$  is a graded lattice (Proposition 4.1), we may apply the  $\mathfrak{C}$ -construction from §6.1 and obtain  $\mathfrak{G}(K|k) := \mathfrak{C}(\mathfrak{G}^*(K|k))$ , the associated set with closure operation. On the other hand,  $\mathfrak{C}(\mathbb{G}^*(K|k)) = \mathbb{G}(K|k)$  is a combinatorial geometry, as described in §6.3. Since  $\Omega_K : \mathbb{G}^*(K|k) \rightarrow \mathfrak{G}^*(K|k)$  is an isomorphism by Proposition 4.1, we see that  $\mathfrak{G}(K|k)$  is also a combinatorial geometry, and that  $\Omega_K$  induces a canonical isomorphism  $\mathbb{G}(K|k) \rightarrow \mathfrak{G}(K|k)$  of combinatorial geometries.
- (4) By Theorem 6.1(1), the field  $K^i$  is uniformly interpretable in  $\mathbb{G}(K|k)$ . Since  $\Omega_K$  induces an isomorphism  $\mathbb{G}(K|k) \rightarrow \mathfrak{G}(K|k)$  of combinatorial geometries, we see that  $K^i$  is (uniformly) interpretable also in  $\mathfrak{G}(K|k)$  using the same interpretation/formulas used to construct  $K^i$  from  $\mathbb{G}(K|k)$ . Finally, we can recover  $k$  as the subset of multiplicatively divisible elements of  $K^i$ .

This completes the proof of Theorem B(1).

*Proof of (2):* We split up the proof of (2) into two steps. In the first step, we trace through the steps from the proof of (1) above to construct a map

$$\underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L)) \rightarrow \text{Isom}_F^i(K, L)$$

which will be our candidate for the inverse of  $\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$ . It will be clear from the construction that this map is a *left inverse*, meaning that the composition

$$\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L)) \rightarrow \text{Isom}_F^i(K, L)$$

is the identity. It will also be clear from the construction that this map is compatible with compositions of isomorphisms on either side; this will allow us to reduce to the case where  $K|k = L|l$ . In the second step, we complete the proof that this candidate is indeed the inverse of the canonical map  $\text{Isom}_F^i(K, L) \rightarrow \underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$ .

### **Step 1: Constructing the inverse.**

First, note that if  $\underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  is non-empty, then the full mod- $\ell$  Milnor K-rings  $k_*^M(K)$  and  $k_*^M(L)$  are isomorphic, since  $k_*^M(K)$  and  $k_*^M(L)$  are quadratic algebras (see Step (1) in the proof of assertion (1) above). Therefore, one has  $\text{tr. deg}(K|k) = \text{tr. deg}(L|l)$ , since  $\text{tr. deg}(K|k) = \dim_K^M(k_1^M(K))$  and  $\text{tr. deg}(L|l) = \dim_L^M(k_1^M(L))$  by Lemmas 3.3 and 3.5. Thus, we can also apply the process from assertion (1) to  $\mathcal{K}_{\text{rat}}^M(L|l)$  to reconstruct  $L^i|l$ . The construction of the map  $\underline{\text{Isom}}_{\text{rat}}^M(k_1^M(K), k_1^M(L)) \rightarrow \text{Isom}_F^i(K, L)$  follows from the observation that this reconstruction process from assertion (1) is compatible with isomorphisms and



invariant under multiplying isomorphisms by  $\epsilon \in (\mathbb{Z}/\ell)^\times$ . The precise construction is outlined in the steps below.

(1) Propositions 5.3 and 5.4 yield a canonical map:

$$\mathrm{Isom}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L)) \rightarrow \mathrm{Isom}^*(\mathfrak{G}^*(K|k), \mathfrak{G}^*(L|l)).$$

It is clear from the construction that this map is compatible with compositions and that it factors through  $\underline{\mathrm{Isom}}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L))$ . Thus, we obtain the first component of our map:

$$\underline{\mathrm{Isom}}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L)) \rightarrow \mathrm{Isom}^*(\mathfrak{G}^*(K|k), \mathfrak{G}^*(L|l)).$$

(2) Proposition 4.1 shows that  $\mathfrak{G}^*(K|k)$  and  $\mathfrak{G}^*(L|l)$  are graded lattices. Denoting  $\mathfrak{G}(K|k) := \mathfrak{C}(\mathfrak{G}^*(K|k))$  and  $\mathfrak{G}(L|l) := \mathfrak{C}(\mathfrak{G}^*(L|l))$  as in step (3) from the proof of (1) above, the  $\mathfrak{C}$ -construction from §6.1 yields a canonical map which is compatible with compositions:

$$\mathrm{Isom}^*(\mathfrak{G}^*(K|k), \mathfrak{G}^*(L|l)) \rightarrow \mathrm{Isom}^{\mathrm{cl}}(\mathfrak{G}(K|k), \mathfrak{G}(L|l)).$$

(3) Proposition 4.1 furthermore shows that  $\Omega_K$  resp.  $\Omega_L$  induce a canonical *bijection* which is compatible with compositions:

$$\mathrm{Isom}^{\mathrm{cl}}(\mathbb{G}(K|k), \mathbb{G}(L|l)) \xrightarrow{\cong} \mathrm{Isom}^{\mathrm{cl}}(\mathfrak{G}(K|k), \mathfrak{G}(L|l)).$$

The next component is the inverse of the map above, which is also a bijection that is compatible with compositions:

$$\mathrm{Isom}^{\mathrm{cl}}(\mathfrak{G}(K|k), \mathfrak{G}(L|l)) \xrightarrow{\cong} \mathrm{Isom}^{\mathrm{cl}}(\mathbb{G}(K|k), \mathbb{G}(L|l)).$$

(4) Theorem 6.1(2) says that the canonical map

$$\mathrm{Isom}_F^i(K, L) \rightarrow \mathrm{Isom}^{\mathrm{cl}}(\mathbb{G}(K|k), \mathbb{G}(L|l))$$

is a *bijection*. Since this map is compatible with compositions, the same holds for its inverse

$$\mathrm{Isom}^{\mathrm{cl}}(\mathbb{G}(K|k), \mathbb{G}(L|l)) \rightarrow \mathrm{Isom}_F^i(K, L)$$

which forms the last component.

Taking the composition of the maps described above, we obtain a map

$$\eta_{K,L} : \underline{\mathrm{Isom}}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L)) \rightarrow \mathrm{Isom}_F^i(K, L)$$

which is the candidate for the inverse of  $\mathrm{Isom}_F^i(K, L) \rightarrow \underline{\mathrm{Isom}}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L))$ . Composing with the canonical map  $\mathrm{Isom}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L)) \rightarrow \underline{\mathrm{Isom}}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L))$ , we obtain another map which will be used in the second step of the proof:

$$\eta_{K,L} : \mathrm{Isom}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L)) \rightarrow \mathrm{Isom}_F^i(K, L).$$

## **Step 2: Completing the proof.**

By tracing through the construction above, it is easy to see that  $\eta_{K,L}$  is a *left inverse* for the canonical map  $\mathrm{Isom}_F^i(K, L) \rightarrow \underline{\mathrm{Isom}}_{\mathrm{rat}}^{\mathrm{M}}(\mathbf{k}_1^{\mathrm{M}}(K), \mathbf{k}_1^{\mathrm{M}}(L))$  which was described in §1.5. As noted above, we also see that  $\eta_{K,L}$  is compatible with compositions of isomorphisms. Namely, if  $K|k$ ,  $L|l$  and  $M|m$  are function fields over algebraically closed fields such that

$\text{char } k, \text{char } l, \text{char } m \neq \ell$  and  $\text{tr. deg}(K|k) \geq 5$ , and if  $f \in \text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$  and  $g \in \text{Isom}_{\text{rat}}^M(k_1^M(L), k_1^M(M))$  are given, then

$$\eta_{K,M}(g \circ f) = \eta_{L,M}(g) \circ \eta_{K,L}(f).$$

Define  $\text{Aut}_F^i(K) := \text{Isom}_F^i(K, K)$  and  $\text{Aut}_{\text{rat}}^M(k_1^M(K)) := \text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(K))$ , both considered as groups under composition. Thus, the construction above yields a *group homomorphism*

$$\eta_K := \eta_{K,K} : \text{Aut}_{\text{rat}}^M(k_1^M(K)) \rightarrow \text{Aut}_F^i(K).$$

To complete the proof of Theorem B(2), it suffices to prove that the kernel of  $\eta_K$  is precisely  $(\mathbb{Z}/\ell)^\times \cdot \mathbf{1}_{k_1^M(K)}$ . It is clear from the construction that  $(\mathbb{Z}/\ell)^\times \cdot \mathbf{1}_{k_1^M(K)}$  is contained in  $\ker \eta_K$ . Thus, the rest of the proof will be devoted to proving the opposite inclusion.

Let  $\Phi$  be an element of  $\ker \eta_K$  which is going to be fixed for the rest of the proof; our goal is to show that there exists some  $\epsilon \in (\mathbb{Z}/\ell)^\times$  such that  $\Phi = \epsilon \cdot \mathbf{1}_{k_1^M(K)}$ . Since  $\eta_K$  factors through the *group isomorphisms* furnished by Proposition 4.1 and Theorem 6.1,

$$\text{Isom}^{\text{cl}}(\mathfrak{G}(K|k), \mathfrak{G}(K|k)) \cong \text{Isom}^{\text{cl}}(\mathbb{G}(K|k), \mathbb{G}(K|k)) \cong \text{Aut}_F^i(K),$$

we see that for all  $A \in \mathfrak{G}^1(K|k)$ , one has  $\Phi A = A$ .

For a valuation  $v$  of  $K$ , we define  $\mathfrak{U}_v := \Omega_K(U_v)$ , the image of the  $v$ -units in  $k_1^M(K)$ . Note that the map  $v : K^\times \rightarrow vK$  induces a canonical isomorphism  $k_1^M(K)/\mathfrak{U}_v \xrightarrow{\cong} vK/\ell$ . We begin by showing that the  $\mathfrak{U}_v$  are  $\Phi$ -invariant for *divisorial* valuations  $v$  of  $K$ .

**Lemma 7.1.** *In the notation above, one has  $\Phi \mathfrak{U}_v = \mathfrak{U}_v$  for all divisorial valuations  $v$  of  $K$ .*

*Proof.* Let  $v$  be a divisorial valuation of  $K$ . Since  $\Phi A = A$  for all  $A \in \mathfrak{G}^1(K|k)$ , it suffices to prove that  $\mathfrak{U}_v$  is generated by the elements  $A$  of  $\mathfrak{G}^1(K|k)$  such that  $A \subset \mathfrak{U}_v$ . Because of this, we see that it suffices to prove that  $U_v$  is generated by  $F^\times$  for  $F \in \mathbb{G}^1(K|k)$  such that  $F^\times \subset U_v$ .

For  $t \in \mathcal{O}_v$ , denote by  $\bar{t}$  the image of  $t$  in  $\kappa(v)$ . Since  $v$  is divisorial, we know that  $k \subset \mathcal{O}_v$ , and thus  $\kappa(v)$  is a field extension of  $k$  in a canonical way. In fact,  $\kappa(v)$  is a function field over  $k$  of transcendence degree  $\text{tr. deg}(K|k) - 1$ .

If  $t \in U_v$  is a  $v$ -unit such that  $\bar{t}$  is transcendental over  $k$ , then the restriction of  $v$  to  $k(t)$  is trivial, since the map  $\mathcal{O}_v \rightarrow \kappa(v)$  sends  $k[t]$  isomorphically onto  $k[\bar{t}]$ . Thus, the restriction of  $v$  to  $\overline{k(t)} \cap K =: \kappa_t \in \mathbb{G}^1(K|k)$  is also trivial since  $\kappa_t$  is a finite extension of  $k(t)$ . Therefore  $\kappa_t^\times \subset U_v$ .

Since  $\text{tr. deg}(K|k) \geq 5$  by assumption, we have  $\text{tr. deg}(\kappa(v)|k) \geq 4$ . Thus, there exist (many) elements  $t \in U_v$  such that  $\bar{t}$  is transcendental over  $k$ , and we fix such an element  $t_0 \in U_v$ . On the other hand, if  $x \in U_v$  is such that  $\bar{x} \in k$ , then  $x \cdot t_0^{-1}$  and  $t_0$  both have transcendental images in  $\kappa(v)$ , and one has  $x = (x \cdot t_0^{-1}) \cdot t_0$ . Therefore, any element of  $U_v$  is a product of (at most two) elements  $t \in U_v$  such that  $\bar{t}$  is transcendental over  $k$ .  $\square$

Now let  $A \in \mathfrak{G}^1(K|k)$  be given. For a divisorial valuation  $v$  of  $K$ , let  $A_v = A \cap \mathfrak{U}_v$  denote the kernel of the canonical map

$$A \hookrightarrow k_1^M(K) \rightarrow k_1^M(K)/\mathfrak{U}_v \cong \mathbb{Z}/\ell.$$

We define:

$$\Delta_A := \{A_v : A_v \neq A\}$$

where  $v$  varies over the divisorial valuations of  $K$ . In particular, for all  $T \in \Delta_A$ , one has  $A/T \cong \mathbb{Z}/\ell$ . Furthermore, since  $\Phi A = A$ , and  $\Phi \mathfrak{U}_v = \mathfrak{U}_v$  for all divisorial valuations  $v$  of  $K$  by Lemma 7.1, we deduce that  $\Phi T = T$  for all  $T \in \Delta_A$ .

Next, we will show that there is a natural correspondence between  $\Delta_A$  and (some of) the divisorial valuations of  $F$  where  $F \in \mathbb{G}^1(K|k)$  is such that  $\Omega_K(F) = A$ .

**Lemma 7.2.** *Let  $A \in \mathfrak{G}^1(K|k)$  be given and let  $F \in \mathbb{G}^1(K|k)$  be such that  $\Omega_K(F) = A$ . Let  $T$  be an element of  $\Delta_A$ . Then there exists a unique divisorial valuation  $w_T$  of  $F$  such that  $\Omega_K(U_{w_T}) = T$ .*

*Proof.* Let  $v$  be a divisorial valuation of  $K$  such that  $T = A_v$ . Let  $w$  be the restriction of  $v$  to  $F$ . Since  $A$  is not contained in  $\mathfrak{U}_v$  by the definition of  $\Delta_A$ , it follows that  $w$  is a non-trivial valuation of  $F$ . Since  $vK = \mathbb{Z}$ , we see that  $wF = \mathbb{Z}$  as well. Moreover, as  $v$  is trivial on  $k$ , the same is true for  $w$ . Hence,  $w$  is a divisorial valuation of  $F$ , since  $F$  is the function field of a curve over  $k$ .

It is clear that  $\Omega_K(U_w)$  is contained in  $T$ . And since  $wF = \mathbb{Z}$ , it follows that  $A/\Omega_K(U_w) \cong \mathbb{Z}/\ell$ . Finally, since  $A/T$  is also isomorphic to  $\mathbb{Z}/\ell$ , it follows that  $\Omega_K(U_w) = T$ .

If  $w'$  is another divisorial valuation of  $F$  such that  $\Omega_K(U_{w'}) = T$ , then  $\Omega_F(U_w) = \Omega_F(U_{w'})$  since  $k_1^M(F) \rightarrow k_1^M(K)$  is injective. Moreover, since  $\Omega_F(U_w) = \Omega_F(U_{w'})$  is a proper subgroup of  $k_1^M(F)$ , it follows that  $U_w \cdot U_{w'}$  is a *proper* subgroup of  $F^\times$ . In particular,  $w$  and  $w'$  must be *dependent* as valuations of  $F$ , for otherwise  $U_w \cdot U_{w'} = F^\times$  by the approximation theorem for independent valuations (cf. [EP05] Theorem 2.4.1). This implies that  $w = w'$  since  $w$  and  $w'$  are divisorial. Hence  $w =: w_T$  is the unique divisorial valuation of  $F$  such that  $\Omega_K(U_w) = T$ .  $\square$

Given a rational subgroup  $A \in \mathfrak{G}_{\text{rat}}^1(K|k)$  and  $F \in \mathbb{G}^1(K|k)$  such that  $\Omega_K(F) = A$ , we say that  $A$  is **good** if *every* divisorial valuation  $w$  of  $F$  is of the form  $w_T$  for some  $T \in \Delta_A$ , where  $w_T$  is as in Lemma 7.2. Similarly, we will say that an element  $t \in K \setminus k$  is **very general** provided that the following two conditions hold:

- (1) The element  $t$  is *general* in  $K$ , in the sense of §5. Recall this implies that  $\Omega_K(k(t))$  is a rational subgroup of  $k_1^M(K)$ .
- (2) The rational subgroup  $\Omega_K(k(t))$  is *good*, as defined above.

Note that if  $t$  is very general in  $K$ , then  $t^{-1}$ ,  $t + a$  and  $t \cdot a$  are also very general in  $K$  for all  $a \in k^\times$ . The following lemma shows that the restriction of  $\Phi$  to any *good* rational subgroup of  $k_1^M(K)$  has the required form.

**Lemma 7.3.** *Let  $A$  be a good rational subgroup of  $k_1^M(K)$ . Then there exists an  $\epsilon_A \in (\mathbb{Z}/\ell)^\times$ , possibly dependent on  $A$ , such that the restriction of  $\Phi$  to  $A$  is precisely  $\epsilon_A \cdot \mathbf{1}_A$ .*

*Proof.* Let  $F \in \mathbb{G}^1(K|k)$  be such that  $\Omega_K(F) = A$ ; note that the canonical map  $F^\times \rightarrow k_1^M(K)$ , whose image is  $A$ , induces an isomorphism  $k_1^M(F) \xrightarrow{\cong} A$ . Let  $\mathfrak{D}_F$  denote the collection of divisorial valuations of  $F$ . Since  $F$  is rational over  $k$ , the multiplicative group  $F^\times/k^\times$  fits into the following short exact sequence:

$$0 \rightarrow F^\times/k^\times \xrightarrow{\text{div}} \bigoplus_{w \in \mathfrak{D}_F} \mathbb{Z} \cdot [w] \xrightarrow{\text{sum}} \mathbb{Z} \rightarrow 0,$$

where  $\text{div}(x) = \sum_{w \in \mathfrak{D}_F} w(x) \cdot [w]$  is the usual divisor map. Since  $k$  is algebraically closed (hence  $k^\times$  is divisible), we see that  $(F^\times/k^\times) \otimes \mathbb{Z}/\ell = k_1^M(F)$ . Since  $\mathbb{Z}$  is torsion-free, we

therefore obtain the following short exact sequence, by tensoring the above exact sequence with  $\mathbb{Z}/\ell$ :

$$0 \rightarrow k_1^M(F) \xrightarrow{\text{div}} \bigoplus_{w \in \mathfrak{D}_F} \mathbb{Z}/\ell \cdot [w] \xrightarrow{\text{sum}} \mathbb{Z}/\ell \rightarrow 0.$$

Since  $A$  is a good rational subgroup, by Lemma 7.2, the map  $w \mapsto \Omega_K(U_w)$  is a *bijection* between  $\mathfrak{D}_F$  and  $\Delta_A$ . Moreover, if  $w \in \mathfrak{D}_F$  is a divisorial valuation of  $F$  and  $T := \Omega_K(U_w) \in \Delta_A$ , then there exists an isomorphism  $\Psi_T : A/T \rightarrow \mathbb{Z}/\ell$  such that the following diagram commutes:

$$\begin{array}{ccccc} F^\times & \xrightarrow{w} & \mathbb{Z} & \xrightarrow{\text{canon.}} & \mathbb{Z}/\ell \\ \downarrow & & & & \parallel \\ A & \xrightarrow{\text{canon.}} & A/T & \xrightarrow{\Psi_T} & \mathbb{Z}/\ell \end{array}$$

In particular, every element of  $A$  is contained in all but at most finitely many  $T \in \Delta_A$ . Thus, we have a canonical map  $\text{div}_A : A \rightarrow \bigoplus_{T \in \Delta_A} A/T$ . Moreover, combining the isomorphisms  $\Psi_T$  for  $T \in \Delta_A$ , and identifying  $\Delta_A$  and  $\mathfrak{D}_F$  via the bijection obtained from Lemma 7.2, we obtain an isomorphism

$$\Psi = (\Psi_T)_T : \bigoplus_{T \in \Delta_A} A/T \rightarrow \bigoplus_{T \in \Delta_A} \mathbb{Z}/\ell \cdot [T]$$

which makes the following diagram commute:

$$\begin{array}{ccc} k_1^M(F) & \xrightarrow{\text{div}} & \bigoplus_{w \in \mathfrak{D}_F} \mathbb{Z}/\ell \cdot [w] = \bigoplus_{T \in \Delta_A} \mathbb{Z}/\ell \cdot [T] \\ \cong \downarrow & & \uparrow \Psi \\ A & \xrightarrow{\text{div}_A} & \bigoplus_{T \in \Delta_A} A/T \end{array}$$

We let  $\text{div}_\ell := \Psi \circ \text{div}_A$ , so that  $\text{div}_\ell$  fits into the following short exact sequence:

$$0 \rightarrow A \xrightarrow{\text{div}_\ell} \bigoplus_{T \in \Delta_A} \mathbb{Z}/\ell \cdot [T] \xrightarrow{\text{sum}} \mathbb{Z}/\ell \rightarrow 0.$$

Next, since  $\Phi A = A$  and  $\Phi T = T$  for all  $T \in \Delta_A$ , it follows that  $\Phi$  induces automorphisms  $\Phi_T : A/T \rightarrow A/T$  for each  $T \in \Delta_A$ , such that  $\text{div}_A \circ \Phi = (\Phi_T)_T \circ \text{div}_A$ . Moreover, for every  $T \in \Delta_A$ , there exists some  $\epsilon_T \in (\mathbb{Z}/\ell)^\times = \text{Aut}(\mathbb{Z}/\ell)$  such that  $\Psi_T \circ \Phi_T = \epsilon_T \cdot \Psi_T$ . In particular, these maps all fit into the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{\text{div}_\ell} & \bigoplus_{T \in \Delta_A} \mathbb{Z}/\ell \cdot [T] & \xrightarrow{\text{sum}} & \mathbb{Z}/\ell \longrightarrow 0 \\ & & \downarrow \Phi & & \downarrow (\epsilon_T)_T & & \parallel \\ 0 & \longrightarrow & A & \xrightarrow{\text{div}_\ell} & \bigoplus_{T \in \Delta_A} \mathbb{Z}/\ell \cdot [T] & \xrightarrow{\text{sum}} & \mathbb{Z}/\ell \longrightarrow 0 \end{array}$$

Let  $T_1, T_2 \in \Delta_A$  be given. Then there exists some  $a \in A$  such that  $\text{div}_\ell(a) = [T_1] - [T_2]$ . But then  $\text{div}_\ell(\Phi(a)) = \epsilon_{T_1} \cdot [T_1] - \epsilon_{T_2} \cdot [T_2]$ , and this implies that  $\epsilon_{T_1} = \epsilon_{T_2}$  by the exactness of the bottom row in the diagram above. Namely, there exists a *single*  $\epsilon_A \in (\mathbb{Z}/\ell)^\times$  such that  $\Psi_T \circ \Phi_T = \epsilon_A \cdot \Psi_T$  for all  $T \in \Delta_A$ . Thus, the injectivity of  $\text{div}_\ell$  in the diagram above implies that the restriction of  $\Phi$  to  $A$  is precisely multiplication by this  $\epsilon_A$ .  $\square$

The conclusion of the proof of Theorem B will rely on the following refinement of Fact 5.1, which can be seen as a “Birational Bertini Theorem” for very general elements.

**Proposition 7.4.** *In the above notation, let  $t_1, t_2$  be elements of  $K$  which are algebraically independent over  $k$  such that  $t_2$  is separable in  $K$ . Then, for all but finitely many  $b \in k$ , the following holds: For all but finitely many  $a \in k$ , the element  $(t_1 + a)/(t_2 + b)$  is very general in  $K$ .*

*Proof.* Extend  $t_1, t_2$  to a transcendence base  $\mathbf{t} = (t_1, \dots, t_d)$  for  $K|k$  and consider  $X_0 = \mathbb{A}_{k, \mathbf{t}}^n$ , affine  $n$ -space over  $k$  with coordinates  $\mathbf{t}$ . Given  $a, b \in k$ , we put  $t_{a,b} := (t_1 + a)/(t_2 + b)$ . The inclusion  $k(t_{a,b}) \hookrightarrow k(\mathbf{t})$  induces a dominant rational map  $\pi_{a,b} : X_0 \rightarrow \mathbb{P}_k^1$ , defined on  $k$ -points by  $(a_1, \dots, a_n) \mapsto (a_1 + a)/(a_2 + b)$ . The inclusion of function fields induced by  $\pi_{a,b}$  is the map  $k(t) \hookrightarrow k(\mathbf{t})$  sending  $t$  to  $t_{a,b}$ , and we will identify  $k(t_{a,b})$  with the function field of  $\mathbb{P}_k^1$ . The fibers of  $X_0 \rightarrow \mathbb{P}_k^1$  over the closed points of  $\mathbb{P}_k^1$  are of the following form:

- (1) For  $c \in \mathbb{A}_k^1(k)$ , the fiber over  $c$  is the linear subvariety of  $X_0$  defined by the equation  $(t_1 + a) = c \cdot (t_2 + b)$ .
- (2) For  $\infty \in \mathbb{P}_k^1(k) \setminus \mathbb{A}_k^1(k)$ , the fiber over  $\infty$  is the linear subvariety of  $X_0$  defined by the equation  $t_2 + b = 0$ .

In particular, the map  $\pi_{a,b}$  is surjective.

By Fact 5.1, we see that for any given  $b \in k$ , the element  $t_{a,b} = t_1/(t_2 + b) + a/(t_2 + b)$  is general in  $K$  for all but finitely many  $a \in k$ . Also, Lemma 3.2 says that all but finitely many prime-divisors of  $X_0$  are  $\ell$ -unramified in  $K$ . Thus, by the discussion above, for all but finitely many  $b \in k$ , the following two conditions hold for all but finitely many  $a \in k$  (the excluded  $a$ 's possibly depending on  $b$ ):

- (1) The element  $t_{a,b}$  is general in  $K$ .
- (2) For any closed point  $x$  of  $\mathbb{P}_k^1$ , the fiber of the map  $\pi_{a,b}$  above  $x$  is  $\ell$ -unramified in  $K$ .

To conclude the proof, we will show that any  $t_{a,b}$  satisfying these two conditions is actually very general in  $K$ . By condition (1), we know that  $t_{a,b}$  is already general in  $K$ . Thus, setting  $A := \Omega_K(k(t_{a,b}))$ , we must show that every divisorial valuation  $w$  of  $k(t_{a,b})$  is of the form  $w_T$  for some  $T \in \Delta_A$ , where  $w_T$  is as described in Lemma 7.2.

Let  $w$  be a divisorial valuation of  $k(t_{a,b})$  and let  $x$  be the unique closed point (i.e. prime-divisor) of  $\mathbb{P}_k^1$  such that  $w = w_x$ . Let  $P_0$  be the generic point of  $(X_0)_x$ , the fiber of  $\pi_{a,b}$  over  $x$ , and let  $v_0 = v_{P_0}$  be the valuation of  $k(\mathbf{t})$  associated to  $P_0$ . Then  $w$  is the restriction of  $v_0$  to  $k(t_{a,b})$ , and  $v_0 k(\mathbf{t}) = w k(t_{a,b})$ .

Let  $X$  denote the normalization of  $X_0$  in  $K$ , and let  $P$  be a prime divisor on  $X$  which prolongs  $P_0$ . Furthermore, let  $v = v_P$  denote the valuation of  $K$  associated to  $P$ . Then  $w$  is the restriction of  $v$  to  $k(t_{a,b})$  and  $v_0$  is the restriction of  $w$  to  $k(\mathbf{t})$ . Furthermore, as  $P_0$  is  $\ell$ -unramified in  $K$ , we see that  $v_0 k(\mathbf{t})$  is not contained in  $\ell \cdot vK$ , and therefore  $w k(t_{a,b})$  is not contained in  $\ell \cdot vK$ . In particular,  $\Omega_K(k(t_{a,b})) = A$  is not contained in  $\mathfrak{U}_v$ . Thus,  $\mathfrak{U}_v \cap A =: T$  is an element of  $\Delta_A$ . Finally, the argument of Lemma 7.2 shows that  $w = w_T$ . Namely, it is clear that  $\Omega_K(U_w) \subset T$ , while both  $A/\Omega_K(U_w)$  and  $A/T$  are isomorphic to  $\mathbb{Z}/\ell$ ; hence  $\Omega_K(U_w) = T$ .  $\square$

By Lemma 7.3, in order to conclude the proof, we must prove the following two assertions:

- (1) That  $k_1^M(K)$  is generated by its good rational subgroups.



- (2) That for any two good rational subgroups  $A, B$  of  $k_1^M(K)$ , one has  $\epsilon_A = \epsilon_B$ , where  $\epsilon_A, \epsilon_B \in (\mathbb{Z}/\ell)^\times$  are as in the statement of Lemma 7.3.

For assertion (1), assume that  $x \in K^\times \setminus k^\times$  is separable in  $K$ . Let  $y$  be an element of  $K^\times$  which is algebraically independent from  $x$ . By Proposition 7.4, there exist  $a, b \in k$  such that both  $(xy - ab)/(x + b)$  and  $(y + a)/(x + b)$  are very general in  $K$ . Therefore,  $(xy + ax)/(x + b) = (xy - ab)/(x + b) + a$  and  $(x + b)/(y + a) = ((y + a)/(x + b))^{-1}$  are also very general in  $K$ . Hence

$$x = \left( \frac{xy + ax}{x + b} \right) \cdot \left( \frac{x + b}{y + a} \right)$$

is a product of two very general elements of  $K$ . Since any non-constant element of  $K$  is a power of an element of  $K$  which is separable in  $K$ , we deduce that  $k_1^M(K)$  is generated by its good rational subgroups.

For assertion (2), assume that  $A$  and  $B$  are two *different* good rational subgroups of  $k_1^M(K)$ , and that  $x, y$  are very general elements of  $K$  such that  $A = \Omega_K(k(x))$  and  $\Omega_K(k(y)) = B$ . Note that  $x, y$  must be algebraically independent over  $k$ . By Proposition 7.4, there exists  $b \in k$  such that for all but finitely many  $a \in k$ , the element  $(x + a)/(y + b)$  is also very general in  $K$ . Since  $k_1^M(k(x)) \rightarrow k_1^M(K)$  is injective, we can choose an  $a \in k$  such that  $(x + a)/(y + b) =: z$  is very general, and such that  $(x + a)$  and  $(y + b)$  have  $\mathbb{Z}/\ell$ -independent images in  $k_1^M(K)$ . Let  $C = \Omega_K(k(z))$ , and let  $\epsilon_A, \epsilon_B, \epsilon_C \in (\mathbb{Z}/\ell)^\times$  be as in Lemma 7.3. Now we calculate in  $k_1^M(K)$ :

$$\frac{(x + a)^{\epsilon_A}}{(y + b)^{\epsilon_B}} = \frac{\Phi(x + a)}{\Phi(y + b)} = \Phi\left(\frac{x + a}{y + b}\right) = \left(\frac{x + a}{y + b}\right)^{\epsilon_C} = \frac{(x + a)^{\epsilon_C}}{(y + b)^{\epsilon_C}}.$$

Since  $(x + a)$  and  $(y + b)$  have independent images in  $k_1^M(K)$ , we deduce that  $\epsilon_A = \epsilon_C = \epsilon_B$ , as required. This completes the proof of Theorem B.

## 8. THE ZASSENHAUSS FILTRATION AND GALOIS COHOMOLOGY

In this section we recall the cohomological framework which allows us to translate between The “Galois variant” of our Main Theorem (Theorem A) and the “Milnor variant” of our Main Theorem (Theorem B). The results in this section are by no means new – they are merely a precise formulation of the well-known fact that the cup-product in mod- $\ell$  cohomology is “dual” to the commutator in the mod- $\ell$  central descending series, combined with the Merkurjev-Suslin Theorem [MS82]. The essential calculations concerning commutators and cup products were first carried out by Labute [Lab67] (see also the exposition in [NSW08] §3.9). These calculations have seen a recent resurgence in [CEM12], [EM11], [EM15], [Top15], especially in connection with the Merkurjev-Suslin Theorem [MS82] and the recent proof of the Bloch-Kato conjecture due to Voevodsky-Rost et al. [Voe11], [Ros98], [Wei09]. Nevertheless, the Merkurjev-Suslin Theorem [MS82] suffices for the considerations in this section, and we summarize the appropriate cohomological and group-theoretical calculations below.

Let  $\mathcal{G}$  be a pro- $\ell$  group. We will denote the mod- $\ell$  cohomology  $H^*(\mathcal{G}, \mathbb{Z}/\ell)$  of  $\mathcal{G}$  simply by  $H^*(\mathcal{G})$ . Recall that the Bockstein morphism

$$\beta : H^1(\mathcal{G}) \rightarrow H^2(\mathcal{G})$$

is defined to be the connecting homomorphism associated to the short exact sequence of coefficient modules  $0 \rightarrow \mathbb{Z}/\ell \rightarrow \mathbb{Z}/\ell^2 \rightarrow \mathbb{Z}/\ell \rightarrow 0$ .

We recall the first two terms in the mod- $\ell$  Zassenhauss filtration of  $\mathcal{G}$ :

- (1)  $\mathcal{G}^{(2)} := [\mathcal{G}, \mathcal{G}] \cdot \mathcal{G}^\ell$ .
- (2) If  $\ell \neq 2$  then  $\mathcal{G}^{(3)} := [\mathcal{G}, \mathcal{G}^{(2)}] \cdot \mathcal{G}^\ell$ .
- (3) If  $\ell = 2$  then  $\mathcal{G}^{(3)} := [\mathcal{G}, \mathcal{G}^{(2)}] \cdot (\mathcal{G}^{(2)})^\ell$ .

We denote the quotient  $\mathcal{G}/\mathcal{G}^{(2)}$  by  $\mathcal{G}^a$  and the quotient  $\mathcal{G}/\mathcal{G}^{(3)}$  by  $\mathcal{G}^c$ . In particular, note that  $\mathcal{G}^a$  is an  $\ell$ -elementary abelian pro- $\ell$  group, and that  $\mathcal{G}^c \rightarrow \mathcal{G}^a$  is a central extension whose kernel is also  $\ell$ -elementary abelian.

For  $\sigma, \tau \in \mathcal{G}^a$ , we define  $[\sigma, \tau] := \tilde{\sigma}^{-1} \tilde{\tau}^{-1} \tilde{\sigma} \tilde{\tau}$  where  $\tilde{\sigma}, \tilde{\tau} \in \mathcal{G}^c$  are some lifts of  $\sigma, \tau \in \mathcal{G}^a$ . Since  $\mathcal{G}^c \rightarrow \mathcal{G}^a$  is a central extension, the element  $[\sigma, \tau] \in \mathcal{G}^{(2)}/\mathcal{G}^{(3)}$  doesn't depend on the choice of lifts  $\tilde{\sigma}, \tilde{\tau}$ .

For a discrete  $\mathbb{Z}/\ell$ -module  $M$ , define  $\wedge^2(M) := M \otimes M / \langle x \otimes x : x \in M \rangle$ . For a pro- $\ell$   $\mathbb{Z}/\ell$ -module  $\mathcal{G}^a$ , we define:

$$\widehat{\wedge}^2(\mathcal{G}^a) := \varprojlim_H \wedge^2(\mathcal{G}^a/H)$$

where  $H$  varies over the open subgroups of  $\mathcal{G}^a$  and thus  $\mathcal{G}^a/H$  is a finite (hence discrete)  $\mathbb{Z}/\ell$ -module.

For a pro- $\ell$   $\mathbb{Z}/\ell$ -module  $\mathcal{G}^a$ , let  $(\mathcal{G}^a)^\vee$  denote the Pontryagin-dual of  $\mathcal{G}^a$ . Namely,  $(\mathcal{G}^a)^\vee := \text{Hom}(\mathcal{G}^a, \mathbb{Z}/\ell)$  is a discrete  $\mathbb{Z}/\ell$ -module. Thus, the canonical perfect pairing  $\mathcal{G}^a \times (\mathcal{G}^a)^\vee \rightarrow \mathbb{Z}/\ell$  induces a perfect pairing of wedge-products:

$$\widehat{\wedge}^2(\mathcal{G}^a) \times \wedge^2((\mathcal{G}^a)^\vee) \rightarrow \mathbb{Z}/\ell$$

which is defined in the usual way by  $(\sigma \wedge \tau) \times (f \wedge g) \mapsto f(\sigma) \cdot g(\tau) - f(\tau) \cdot g(\sigma)$ .

**8.1. A presentation of  $H^2$ .** Since  $\mathcal{G}^a$  is isomorphic to a direct power of  $\mathbb{Z}/\ell$ , the Künneth formula for (profinite) group cohomology, together with the well-known structure of the cohomology ring  $H^*(\mathbb{Z}/\ell, \mathbb{Z}/\ell)$ , yield the following fact. See [EM11] §2.D, and/or [Top15] Lemma 2.1 for more details.

**Fact 8.1.** *In the notation above, the canonical map*

$$\begin{aligned} (H^1(\mathcal{G}^a) \otimes H^1(\mathcal{G}^a)) \oplus H^1(\mathcal{G}^a) &\longrightarrow H^2(\mathcal{G}^a) \\ (x \otimes y) \oplus z &\longmapsto x \cup y + \beta z \end{aligned}$$

*is surjective, and the kernel of this map is generated by all elements of the form  $(x \otimes x) \oplus \binom{\ell}{2} \cdot x$  for  $x$  varying in  $H^1(\mathcal{G}^a)$ .*

Thus, if  $\ell \neq 2$ , then the map  $\wedge^2(H^1(\mathcal{G}^a)) \oplus H^1(\mathcal{G}^a) \rightarrow H^2(\mathcal{G}^a)$ , defined by  $(x \wedge y) \oplus z \mapsto x \cup y + \beta z$ , is an isomorphism. On the other hand, if  $\ell = 2$ , then the cup product map yields an isomorphism  $\text{Sym}^2(H^1(\mathcal{G}^a)) \rightarrow H^2(\mathcal{G}^a)$ , where  $\text{Sym}^2$  denotes the second symmetric power.

The decomposable part of  $H^2(\mathcal{G}^a)$ , denoted  $H^2(\mathcal{G}^a)_{\text{dec}}$ , is defined as the image of the cup product  $H^1(\mathcal{G}^a) \otimes H^1(\mathcal{G}^a) \rightarrow H^2(\mathcal{G}^a)$ . Thus, if  $\ell \neq 2$ , then the cup product yields an isomorphism  $\wedge^2(H^1(\mathcal{G}^a)) \rightarrow H^2(\mathcal{G}^a)_{\text{dec}}$ . On the other hand, if  $\ell = 2$ , then  $H^2(\mathcal{G}^a) = H^2(\mathcal{G}^a)_{\text{dec}}$ .

**8.2. Cup-products and the Zassenhauss filtration.** Since the inflation map  $H^1(\mathcal{G}^a) \rightarrow H^1(\mathcal{G})$  is an isomorphism, we see that the Lyndon-Hochschild-Serre spectral sequence associated to the extension  $\mathcal{G} \rightarrow \mathcal{G}^a$  yields an exact sequence:

$$(8.1) \quad 0 \rightarrow H^1(\mathcal{G}^{(2)})^{\mathcal{G}} \xrightarrow{d_2} H^2(\mathcal{G}^a) \xrightarrow{\text{inf}} H^2(\mathcal{G}),$$

where  $d_2 := d_2^{0,1}$  is the associated differential on the  $E_2$ -page of the spectral sequence. The map  $d_2$  above also agrees with the *transgression map* (cf. [NSW08] Theorem 2.4.3). Also, note that  $H^1(\mathcal{G}^{(2)})^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(\mathcal{G}^{(2)}, \mathbb{Z}/\ell)$  is the set of  $\mathcal{G}$ -equivariant homomorphisms  $\mathcal{G}^{(2)} \rightarrow \mathbb{Z}/\ell$ , where  $\mathcal{G}$  acts on  $\mathcal{G}^{(2)}$  by conjugation and trivially on  $\mathbb{Z}/\ell$ . Since  $\mathcal{G}^c \rightarrow \mathcal{G}^a$  is a central extension with kernel  $\mathcal{G}^{(2)}/\mathcal{G}^{(3)}$  which is killed by  $\ell$ , we obtain a canonical *injective* map:

$$(\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^{\vee} \hookrightarrow H^1(\mathcal{G}^{(2)})^{\mathcal{G}}.$$

The following lemma describes the image of this injection with respect to  $d_2$ . This lemma is essentially identical to [EM15] Corollary 10.9, but we still provide a detailed proof to keep the discussion as self-contained as possible.

**Lemma 8.2.** *The image of the canonical injective map  $(\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^{\vee} \hookrightarrow H^1(\mathcal{G}^{(2)})^{\mathcal{G}}$  is precisely  $d_2^{-1}(H^2(\mathcal{G}^a)_{\text{dec}})$ , the preimage of the decomposable part of  $H^2(\mathcal{G}^a)$  under the map  $d_2 : H^1(\mathcal{G}^{(2)})^{\mathcal{G}} \rightarrow H^2(\mathcal{G}^a)$ .*

*Proof.* Let  $\mathcal{G}^{[3]} := [\mathcal{G}, \mathcal{G}^{(2)}] \cdot (\mathcal{G}^{(2)})^{\ell}$  denote the third term in the mod- $\ell$  central descending series. I.e.  $\mathcal{G}^{[3]}$  is the left-kernel of the canonical pairing  $\mathcal{G}^{(2)} \times H^1(\mathcal{G}^{(2)})^{\mathcal{G}} \rightarrow \mathbb{Z}/\ell$  (see e.g. [EM11] §2.A). In other words, we may identify the following three groups:

$$H^1(\mathcal{G}^{(2)})^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(\mathcal{G}^{(2)}, \mathbb{Z}/\ell) = (\mathcal{G}^{(2)}/\mathcal{G}^{[3]})^{\vee}.$$

Moreover, note that one has  $\mathcal{G}^{[3]} \subset \mathcal{G}^{(3)}$ . If  $\ell \neq 2$ , then  $\mathcal{G}^{(3)}$  is (topologically) generated by  $\mathcal{G}^{[3]}$  and  $\mathcal{G}^{\ell}$ . On the other hand, if  $\ell = 2$ , then  $\mathcal{G}^{[3]} = \mathcal{G}^{(3)}$  by definition.

*Case  $\ell = 2$ :* In this case, one has  $\mathcal{G}^{[3]} = \mathcal{G}^{(3)}$  and thus  $(\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^{\vee} = H^1(\mathcal{G}^{(2)})^{\mathcal{G}}$ . Also, Fact 8.1 implies that  $H^2(\mathcal{G}^a)_{\text{dec}} = H^2(\mathcal{G}^a)$ . Thus, the lemma follows trivially.

*Case  $\ell \neq 2$ :* Fact 8.1 implies that the map  $\wedge^2(H^1(\mathcal{G}^a)) \oplus H^1(\mathcal{G}^a) \rightarrow H^2(\mathcal{G}^a)$ , given by  $(x \wedge y) \oplus z \mapsto x \cup y + \beta z$ , is an isomorphism. In particular, any element  $\eta \in H^2(\mathcal{G}^a)$  can be represented as

$$\eta = \left( \sum_i x_i \cup y_i \right) + \beta z$$

for some  $x_i, y_i, z \in H^1(\mathcal{G}^a)$ , with  $z$  uniquely determined by  $\eta$ . Also, note that  $\eta \in H^2(\mathcal{G}^a)_{\text{dec}}$  if and only if  $z = 0$ .

Next, recall that  $\mathcal{G}^{(3)}$  is (topologically) generated by  $\mathcal{G}^{[3]}$  and  $\mathcal{G}^{\ell}$ . Thus, the image of the injection  $(\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^{\vee} \hookrightarrow H^1(\mathcal{G}^{(2)})^{\mathcal{G}}$  consists precisely of the elements

$$f \in H^1(\mathcal{G}^{(2)})^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(\mathcal{G}^{(2)}, \mathbb{Z}/\ell) = (\mathcal{G}^{(2)}/\mathcal{G}^{[3]})^{\vee}$$

such that  $f(\tilde{\sigma}^{\ell}) = 0$  for all  $\tilde{\sigma} \in \mathcal{G}$ .

Now let  $f \in H^1(\mathcal{G}^{(2)})^{\mathcal{G}}$  be given. By the observation above using Fact 8.1, there exists a representation of  $d_2 f$  of the form

$$d_2 f = \left( \sum_i x_i \cup y_i \right) + \beta z$$

for some  $x_i, y_i, z \in H^1(\mathcal{G}^a) = \text{Hom}(\mathcal{G}^a, \mathbb{Z}/\ell)$ , with  $z$  uniquely determined by  $d_2 f$ . Let  $\tilde{\sigma} \in \mathcal{G}$  be given with image  $\sigma \in \mathcal{G}^a$ . Then [NSW08] Proposition 3.9.14 (see also [Top15] Theorem 2) implies that  $-f(\tilde{\sigma}^{\ell}) = z(\sigma)$ . Thus, the description above shows that  $f$  is in the image of

$(\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^\vee \hookrightarrow H^1(\mathcal{G}^{(2)})^\mathcal{G}$  if and only if  $z(\sigma) = 0$  for all  $\sigma \in \mathcal{G}^a$ , i.e.  $z = 0$  in  $H^1(\mathcal{G}^a)$ . As discussed above, this is further equivalent to  $d_2 f \in H^2(\mathcal{G}^a)_{\text{dec}}$ , as required.  $\square$

We now recall the well-known duality between the map  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}^a) \rightarrow \mathcal{G}^{(2)}/\mathcal{G}^{(3)}$  and cup-products in mod- $\ell$  cohomology. By Fact 8.1, we note that the cup product induces a canonical isomorphism

$$\wedge^2(H^1(\mathcal{G}^a)) \xrightarrow{\cong} H^2(\mathcal{G}^a)_{\text{dec}}/(\beta H^1(\mathcal{G}^a) \cap H^2(\mathcal{G}^a)_{\text{dec}}).$$

We will henceforth identify these two groups via this isomorphism. Next, note that the map  $d_2 : H^1(\mathcal{G}^{(2)})^\mathcal{G} \rightarrow H^2(\mathcal{G}^a)$  restricts to a map  $d_2 : (\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^\vee \rightarrow H^2(\mathcal{G}^a)_{\text{dec}}$  by Lemma 8.2. Therefore, we obtain an induced map

$$\Upsilon : (\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^\vee \xrightarrow{-d_2} H^2(\mathcal{G}^a)_{\text{dec}} \rightarrow \wedge^2(H^1(\mathcal{G}^a))$$

where the surjective map on the right is induced by the identification we made above. Note that we have replaced  $d_2$  with  $-d_2$  in the definition of  $\Upsilon$ , in order to account for the negative sign that appears in the results referenced below. With this notation, the following fact follows immediately from [NSW08] Proposition 3.9.13 and/or [Top15] Theorem 2(1).

**Fact 8.3.** *The map  $\Upsilon : (\mathcal{G}^{(2)}/\mathcal{G}^{(3)})^\vee \rightarrow \wedge^2(H^1(\mathcal{G}^a))$  defined above is precisely the dual of the commutator map  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}^a) \rightarrow \mathcal{G}^{(2)}/\mathcal{G}^{(3)}$ .*

**8.3. Galois cohomology and Kummer theory.** Suppose that  $K$  is a field such that  $\text{char } K \neq \ell$  and  $\mu_{\ell^2} \subset K$ . Recall that  $K(\ell)$  denotes the maximal pro- $\ell$  Galois extension of  $K$  and that  $\mathcal{G}_K := \text{Gal}(K(\ell)|K)$  denotes the maximal pro- $\ell$  Galois group of  $K$ . Furthermore, recall that Kummer theory yields a canonical perfect pairing:

$$\mathcal{G}_K^a \times k_1^M(K) \rightarrow \mu_\ell,$$

which is defined by  $(\sigma, x) \mapsto \sigma \sqrt[\ell]{x} / \sqrt[\ell]{x}$ .

Choose a primitive  $\ell$ -th root of unity  $\omega \in \mu_\ell \subset K$ , and consider the induced isomorphism  $\mu_\ell \cong \mathbb{Z}/\ell$  given by  $\omega^i \mapsto i$ . We therefore obtain an induced perfect pairing:

$$(\bullet, \bullet)_\omega : \mathcal{G}_K^a \times k_1^M(K) \rightarrow \mathbb{Z}/\ell$$

where  $(\sigma, x)_\omega = i$  if and only if  $\sigma \sqrt[\ell]{x} / \sqrt[\ell]{x} = \omega^i$ . In particular, the map  $k_1^M(K) \rightarrow H^1(\mathcal{G}_K^a)$ , defined by  $x \mapsto (\bullet, x)_\omega \in H^1(\mathcal{G}_K^a)$ , is an isomorphism of discrete  $\mathbb{Z}/\ell$ -modules.

Recall that the Merkurjev-Suslin theorem [MS82] states that the canonical map  $k_2^M(K) \rightarrow H^2(K, \mu_\ell^{\otimes 2})$  is an isomorphism. In particular, the cup-product map  $H^1(K, \mu_\ell) \otimes H^1(K, \mu_\ell) \rightarrow H^2(K, \mu_\ell^{\otimes 2})$  is surjective. Our choice of isomorphism  $\mu_\ell \cong \mathbb{Z}/\ell$  given by  $\omega$  induces a compatible isomorphism  $\mu_\ell^{\otimes 2} \cong \mathbb{Z}/\ell$ . In particular, the cup-product map  $H^1(G_K) \otimes H^1(G_K) \rightarrow H^2(G_K)$  is surjective as well. On the other hand, the inflation map  $H^1(\mathcal{G}_K^a) \rightarrow H^1(G_K)$  is an isomorphism. From this, it follows that the inflation map  $H^2(\mathcal{G}_K^a) \rightarrow H^2(G_K)$  is surjective. Hence the inflation map  $H^2(\mathcal{G}_K) \rightarrow H^2(G_K)$  is surjective as well. This observation allows us to work with  $\mathcal{G}_K$  instead of  $G_K$  via the following fact. See also [CEM12] Remark 8.2.

**Fact 8.4.** *In the context above, the inflation map  $H^2(\mathcal{G}_K) \rightarrow H^2(G_K)$  is an isomorphism.*

*Proof.* Surjectivity of this map was discussed above. Since  $K(\ell)^\times$  is  $\ell$ -divisible, it follows that  $H^1(G_{K(\ell)}) \cong H^1(K(\ell), \mu_\ell) = k_1^M(K(\ell)) = 0$ . Thus the map  $H^2(\mathcal{G}_K) \rightarrow H^2(G_K)$  is injective since its kernel is the image of  $d_2 : H^1(G_{K(\ell)})^{\mathcal{G}_K} \rightarrow H^2(\mathcal{G}_K)$ .  $\square$

For the rest of the section, we will (canonically) identify  $H^2(\mathcal{G}_K)$  and  $H^2(G_K)$  using Fact 8.4. Next we discuss the Bockstein morphism in Galois cohomology. The following lemma shows the triviality of the Bockstein morphism in the presence of sufficiently many roots of unity. It is possible to deduce the following lemma using the description of the Bockstein morphism in Galois cohomology as a cup-product; see for example [EM11] Proposition 2.6 and/or [Top15] Lemma 4.1. However, the elegant proof that we give below was graciously suggested to us by the referee.

**Lemma 8.5.** *Let  $K$  be a field of characteristic  $\neq \ell$  such that  $\mu_{\ell^2} \subset K$ . Then the Bockstein morphism  $\beta : H^1(\mathcal{G}_K) \rightarrow H^2(\mathcal{G}_K)$  is trivial.*

*Proof.* By choosing compatible isomorphisms  $\mu_{\ell} \cong \mathbb{Z}/\ell$  and  $\mu_{\ell^2} \cong \mathbb{Z}/\ell^2$  of  $G_K$ -modules, Kummer theory shows that the map

$$H^1(\mathcal{G}_K, \mathbb{Z}/\ell^2) \rightarrow H^1(\mathcal{G}_K, \mathbb{Z}/\ell)$$

is surjective as it corresponds to the projection  $K^{\times}/\ell^2 \rightarrow K^{\times}/\ell$ . The mere definition of the Bockstein morphism  $\beta : H^1(\mathcal{G}_K) \rightarrow H^2(\mathcal{G}_K)$  as a connecting morphism shows that the image of the (surjective) map  $H^1(\mathcal{G}_K, \mathbb{Z}/\ell^2) \rightarrow H^1(\mathcal{G}_K)$  is the kernel of  $\beta$ .  $\square$

Recall that the cup product induces a canonical isomorphism, as noted above

$$\wedge^2(H^1(\mathcal{G}_K^a)) = H^2(\mathcal{G}_K^a)_{\text{dec}}/(\beta H^1(\mathcal{G}_K^a) \cap H^2(\mathcal{G}_K^a)_{\text{dec}}).$$

Therefore, if  $\mu_{\ell^2} \subset K$ , we deduce from Lemma 8.5 that the inflation map  $H^2(\mathcal{G}_K^a)_{\text{dec}} \rightarrow H^2(\mathcal{G}_K)$  factors through  $\wedge^2(H^1(\mathcal{G}_K^a))$  and that the induced map  $\wedge^2(H^1(\mathcal{G}_K^a)) \rightarrow H^2(\mathcal{G}_K)$  is the inflation composed with the cup-product:

$$\wedge^2(H^1(\mathcal{G}_K^a)) \xrightarrow{\text{inf}} \wedge^2(H^1(\mathcal{G}_K)) \xrightarrow{\cup} H^2(\mathcal{G}_K).$$

We note that the perfect pairing  $(\bullet, \bullet)_{\omega} : \mathcal{G}_K^a \times k_1^M(K) \rightarrow \mathbb{Z}/\ell$  induces a perfect pairing on wedge-products:

$$(\bullet, \bullet)_{\omega} : \widehat{\wedge}^2(\mathcal{G}_K^a) \times \wedge^2(k_1^M(K)) \rightarrow \mathbb{Z}/\ell.$$

On the one hand, note that the commutator  $[\bullet, \bullet]$  defined above yields a canonical map  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}_K^a) \rightarrow \mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)} =: \mathfrak{Z}_K$ , whose image is denoted by  $\mathfrak{Z}_K^0$ , as defined in §1.2. On the other hand, the product-map on mod- $\ell$  Milnor K-theory yields a surjective map  $\{\bullet, \bullet\} : \wedge^2(k_1^M(K)) \rightarrow k_2^M(K)$ , since  $-1 \in K^{\times \ell}$  and thus  $\{x, x\} = \{x, -1\} = 0$  for all  $x \in k_1^M(K)$  (cf. [GS06] Lemma 7.1.2). The following theorem relates these two maps.

**Theorem 8.6.** *Let  $K$  be a field of characteristic  $\neq \ell$  such that  $\mu_{\ell^2} \subset K$ . Let  $\omega$  be a primitive  $\ell$ -th root of unity in  $K$ . Let  $R$  denote the kernel of the map  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}_K^a) \rightarrow \mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)}$ . Then the inclusion  $R \hookrightarrow \widehat{\wedge}^2(\mathcal{G}_K^a)$  is  $(\bullet, \bullet)_{\omega}$ -dual to the (surjective) product map  $\wedge^2(k_1^M(K)) \rightarrow k_2^M(K)$ .*

*Proof.* Note that the Merkurjev-Suslin Theorem [MS82] implies that the map  $\cup \circ \text{inf} : H^1(\mathcal{G}_K^a) \otimes H^1(\mathcal{G}_K^a) \rightarrow H^2(\mathcal{G}_K)$  is surjective (see the discussion for Fact 8.4). This observation, combined with Lemma 8.2, yields the following commutative diagram with exact



rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & (\mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)})^\vee & \xrightarrow{-d_2} & H^2(\mathcal{G}_K^a)_{\text{dec}} & \xrightarrow{\text{inf}} & H^2(\mathcal{G}_K) \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \parallel \\
0 & \longrightarrow & H^1(\mathcal{G}_K^{(2)})^{\mathcal{G}_K} & \xrightarrow{-d_2} & H^2(\mathcal{G}_K^a) & \xrightarrow{\text{inf}} & H^2(\mathcal{G}_K) \longrightarrow 0
\end{array}$$

Note that we have replaced  $d_2$  with  $-d_2$  in the diagram above in order to account for the negative sign that appears in the definition of  $\Upsilon$  above. As discussed above, we will identify  $H^2(\mathcal{G}_K^a)_{\text{dec}}/(\beta H^1(\mathcal{G}_K^a) \cap H^2(\mathcal{G}_K^a)_{\text{dec}}) = \wedge^2(H^1(\mathcal{G}_K^a))$  using Fact 8.1, and we will consider the map induced by  $-d_2$ :

$$\Upsilon : (\mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)})^\vee \xrightarrow{-d_2} H^2(\mathcal{G}_K^a)_{\text{dec}} \twoheadrightarrow \wedge^2(H^1(\mathcal{G}_K^a)).$$

Since the map  $H^2(\mathcal{G}_K^a)_{\text{dec}} \rightarrow H^2(\mathcal{G}_K)$  factors through  $H^2(\mathcal{G}_K^a)_{\text{dec}}/(\beta H^1(\mathcal{G}_K^a) \cap H^2(\mathcal{G}_K^a)_{\text{dec}}) = \wedge^2(H^1(\mathcal{G}_K^a))$  (see the discussion following Lemma 8.5), we obtain an induced exact sequence:

$$(8.2) \quad (\mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)})^\vee \xrightarrow{\Upsilon} \wedge^2(H^1(\mathcal{G}_K^a)) \xrightarrow{\cup \text{inf}} H^2(\mathcal{G}_K) \rightarrow 0.$$

By Fact 8.3, we see that this map  $\Upsilon : (\mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)})^\vee \rightarrow \wedge^2(H^1(\mathcal{G}_K^a))$  is precisely the dual of  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}_K^a) \rightarrow \mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)}$ . In particular, the  $\mathbb{Z}/\ell$ -dual of (8.2) is none other than

$$0 \rightarrow R \rightarrow \widehat{\wedge}^2(\mathcal{G}_K^a) \xrightarrow{[\bullet, \bullet]} \mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)}.$$

Thus, we have a canonical isomorphism  $R^\vee \cong H^2(\mathcal{G}_K)$  which is compatible with the corresponding maps from  $\wedge^2(H^1(\mathcal{G}_K^a))$  in the obvious sense.

To conclude the theorem, we simply recall that Kummer theory, along with our choice of  $\omega$ , induces an isomorphism  $k_1^M(K) \rightarrow H^1(\mathcal{G}_K^a)$ , which is given by  $x \mapsto (\bullet, x)_\omega$ . We therefore obtain an induced isomorphism  $\wedge^2(k_1^M(K)) \rightarrow \wedge^2(H^1(\mathcal{G}_K^a))$  which is exhibited by the fact that  $\wedge^2(k_1^M(K))$  is  $(\bullet, \bullet)_\omega$ -dual to  $\widehat{\wedge}^2(\mathcal{G}_K^a)$ . Our choice of  $\omega$  induces an isomorphism  $k_2^M(K) \rightarrow H^2(\mathcal{G}_K)$  by the Merkurjev-Suslin theorem [MS82] and Fact 8.4. Furthermore, the multiplication maps are compatible in the sense that the following diagram is commutative:

$$\begin{array}{ccc}
\wedge^2(k_1^M(K)) & \xrightarrow{\{\bullet, \bullet\}} & k_2^M(K) \\
\cong \downarrow & & \downarrow \cong \\
\wedge^2(H^1(\mathcal{G}_K^a)) & \xrightarrow{\cup \text{inf}} & H^2(\mathcal{G}_K)
\end{array}$$

Since  $\wedge^2(H^1(\mathcal{G}_K^a)) \twoheadrightarrow H^2(\mathcal{G}_K)$  is dual to the inclusion  $R \hookrightarrow \widehat{\wedge}^2(\mathcal{G}_K^a)$ , we see that this inclusion  $R \hookrightarrow \widehat{\wedge}^2(\mathcal{G}_K^a)$  is  $(\bullet, \bullet)_\omega$ -dual to the (surjective) multiplication map  $\{\bullet, \bullet\} : \wedge^2(k_1^M(K)) \twoheadrightarrow k_2^M(K)$ , as required.  $\square$

## 9. PROOF OF THEOREM A

We will use the notation of Theorem A. Namely,  $K|k$  and  $L|l$  are function fields over algebraically closed fields such that  $\text{char } k, \text{char } l \neq \ell$  and  $\text{tr. deg}(K|k) \geq 5$ .

*Proof of (1):* Define  $\mathfrak{k}_1 := \text{Hom}(\mathcal{G}_K^a, \mathbb{Z}/\ell)$ . Let  $R$  denote the kernel of  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}_K^a) \rightarrow \mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)} = \mathfrak{Z}_K$  and define  $\mathfrak{k}_2 := \text{Hom}(R, \mathbb{Z}/\ell)$ . The dual of the (injective) map  $R \hookrightarrow \widehat{\wedge}^2(\mathcal{G}_K^a)$  is a surjective map

$$\mu : \wedge^2(\mathfrak{k}_1) = \text{Hom}(\widehat{\wedge}^2(\mathcal{G}_K^a), \mathbb{Z}/\ell) \twoheadrightarrow \text{Hom}(R, \mathbb{Z}/\ell) = \mathfrak{k}_2.$$

Finally, for each quotient  $\pi_H : \mathcal{G}_K^a \twoheadrightarrow \mathcal{G}_K^a/H$  in  $\mathfrak{R}_{\text{rat}}(K|k)$ , let  $A_H$  denote the image of the dual map  $\text{Hom}(\mathcal{G}_K^a/H, \mathbb{Z}/\ell) \hookrightarrow \text{Hom}(\mathcal{G}_K^a, \mathbb{Z}/\ell) = \mathfrak{k}_1$ , and let  $\mathfrak{R}_{\text{rat}}^\vee$  denote the collection  $(A_H)_{\pi_H}$  of these subgroups of  $\mathfrak{k}_1$ , as  $\pi_H$  varies over the elements of  $\mathfrak{R}_{\text{rat}}(K|k)$ . To summarize, we have constructed the following data  $\mathfrak{K}$ :

- Two abelian groups  $\mathfrak{k}_1$  and  $\mathfrak{k}_2$ .
- A surjective homomorphism  $\mu : \wedge^2(\mathfrak{k}_1) \twoheadrightarrow \mathfrak{k}_2$ .
- A collection  $\mathfrak{R}_{\text{rat}}^\vee$  of subgroups of  $\mathfrak{k}_1$ .

Let  $\omega$  be a primitive  $\ell$ -th root of unity in  $K$ , which induces an isomorphism of  $G_K$ -modules  $\mu_\ell \cong \mathbb{Z}/\ell$ . By Kummer theory,  $\omega$  induces an isomorphism  $k_1^M(K) \cong \mathfrak{k}_1$ . Also, by Theorem 8.6, we see that  $\omega$  induces an isomorphism  $k_2^M(K) \cong \mathfrak{k}_2$ , and that the multiplication map  $k_1^M(K) \otimes k_1^M(K) \twoheadrightarrow k_2^M(K)$  corresponds to the composition  $\mathfrak{k}_1 \otimes \mathfrak{k}_1 \twoheadrightarrow \wedge^2(\mathfrak{k}_1) \xrightarrow{\mu} \mathfrak{k}_2$  via these isomorphisms. Finally, Kummer theory again shows that the isomorphism  $k_1^M(K) \cong \mathfrak{k}_1$  sends the elements of  $\mathfrak{G}_{\text{rat}}^1(K|k)$  bijectively onto  $\mathfrak{R}_{\text{rat}}^\vee$ . By Theorem B(1), we know how to reconstruct  $K^i|k$  from the data  $\mathcal{K}_{\text{rat}}^M(K|k)$ , and thus the discussion above shows how to reconstruct  $K^i|k$  from the data  $\mathfrak{K}$ , hence from  $\mathcal{G}_K^c$  together with  $\mathfrak{R}_{\text{rat}}(K|k)$ .

*Proof of (2):* Assume that  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  is non-empty. We first prove that  $\text{char } L \neq \ell$ . Assume the contrary, and recall that this implies that  $\mathcal{G}_L$  is a free pro- $\ell$  group. Thus, one has  $H^2(\mathcal{G}_L) = 0$ . By (8.1), Lemma 8.2 and Fact 8.3, this implies that the canonical map

$$[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}_L^a) \rightarrow \mathcal{G}_L^{(2)}/\mathcal{G}_L^{(3)}$$

is *injective*. On the other hand, since  $\text{Isom}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$  is non-empty, the same condition holds for  $\mathcal{G}_K^a$ . Namely, the map  $[\bullet, \bullet] : \widehat{\wedge}^2(\mathcal{G}_K^a) \rightarrow \mathcal{G}_K^{(2)}/\mathcal{G}_K^{(3)}$  is injective as well. By Theorem 8.6, this implies that  $k_2^M(K) = 0$ , which contradicts Lemma 3.5. Hence  $\text{char } L \neq \ell$ .

To conclude, we must show that the canonical map

$$\text{Isom}_F^i(K, L) \rightarrow \text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a)$$

is a bijection. Choose a primitive  $\ell$ -th root of unity  $\omega_K$  in  $K$  and a primitive  $\ell$ -th root of unity  $\omega_L$  in  $L$ . With these choices made and arguing as in the proof of (1) above, Theorem 8.6 shows that the Kummer pairing yields a *bijection*

$$\Psi_{\omega_K, \omega_L} : \text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L)) \rightarrow \text{Isom}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a).$$

More precisely, for  $\phi \in \text{Isom}_{\text{rat}}^M(k_1^M(K), k_1^M(L))$ , the isomorphism  $\Psi_{\omega_K, \omega_L}(\phi) : \mathcal{G}_L^a \rightarrow \mathcal{G}_K^a$  is defined explicitly by the condition that (using the notation of §8.3):

$$(\sigma, \phi(x))_{\omega_L} = (\Psi_{\omega_K, \omega_L}(\phi)(\sigma), x)_{\omega_K}$$

for all  $\sigma \in \mathcal{G}_L^a$  and  $x \in k_1^M(K)$ . In the terminology of §1.4 and §1.5, it follows from Kummer theory that  $\phi$  is compatible with  $\mathfrak{G}_{\text{rat}}^1$  if and only if  $\Psi_{\omega_K, \omega_L}(\phi)$  is compatible with  $\mathfrak{R}_{\text{rat}}$ . Also, in the terminology of §1.2 and §1.5, it follows from Theorem 8.6 that  $\phi$  is compatible with  $k_2^M$  if and only if  $\Psi_{\omega_K, \omega_L}(\phi)$  is compatible with  $[\bullet, \bullet]$ .

Note that the map  $\Psi_{\omega_K, \omega_L}$  depends on the choices of  $\omega_K$  and  $\omega_L$ . Nevertheless, changing  $\omega_K$  and/or  $\omega_L$  has the effect of replacing  $\Psi_{\omega_K, \omega_L}$  by  $\epsilon \cdot \Psi_{\omega_K, \omega_L}$  for some  $\epsilon \in (\mathbb{Z}/\ell)^\times$ . Therefore, we obtain a *canonical* bijection on  $(\mathbb{Z}/\ell)^\times$ -equivalence classes which is completely independent from choosing roots of unity:

$$\underline{\text{Isom}}_{\text{rat}}^{\text{M}}(k_1^{\text{M}}(K), k_1^{\text{M}}(L)) \xrightarrow{\cong} \underline{\text{Isom}}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a).$$

Furthermore, by Kummer theory, this bijection is compatible with the canonical maps from  $\text{Isom}_F^i(K, L)$  in the sense that the following diagram commutes:

$$\begin{array}{ccc} & \underline{\text{Isom}}_{\text{rat}}^{\text{M}}(k_1^{\text{M}}(K), k_1^{\text{M}}(L)) & \\ \text{canon.} \nearrow & \downarrow \cong & \\ \text{Isom}_F^i(K, L) & & \underline{\text{Isom}}_{\text{rat}}^c(\mathcal{G}_L^a, \mathcal{G}_K^a) \\ \text{canon.} \searrow & & \end{array}$$

Thus, Theorem A(2) follows from Theorem B(2).

## REFERENCES

- [Art57] E. Artin, *Geometric algebra*, Interscience Publishers (New York), 1957. ↑3
- [Bog91] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Algebraic geometry and analytic geometry (Tokyo, 1990), 1991, pp. 26–52. MR1260938 (94k:14013) ↑1, 3
- [BT02] F. A. Bogomolov and Y. Tschinkel, *Commuting elements of Galois groups of function fields*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), 2002, pp. 75–120. ↑4, 6
- [BT08] ———, *Reconstruction of function fields*, Geom. Funct. Anal. **18** (2008), no. 2, 400–462. MR2421544 (2009g:11155) ↑3
- [BT09] ———, *Milnor  $K_2$  and field homomorphisms*, Surveys in differential geometry. Vol. XIII. Geometry, analysis, and algebraic geometry: forty years of the Journal of Differential Geometry, 2009, pp. 223–244. MR2537087 (2010j:19005) ↑8
- [BT11] ———, *Reconstruction of higher-dimensional function fields*, Mosc. Math. J. **11** (2011), no. 2, 185–204, 406. MR2859233 ↑3
- [BT12] ———, *Introduction to birational anabelian geometry.*, Current developments in algebraic geometry. Selected papers based on the presentations at the workshop “Classical algebraic geometry today”, MSRI, Berkeley, CA, USA, January 26–30, 2009, 2012, pp. 17–63 (English). ↑2, 7
- [CEM12] K. S. Chebolu, I. Efrat, and J. Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Mathematische Annalen **352** (May 2012), no. 1, 205–221, available at <http://www.arxiv.org/abs/0905.1364>. ↑34, 37
- [EH91] D. M. Evans and E. Hrushovski, *Projective planes in algebraically closed fields*, Proc. London Math. Soc. (3) **62** (1991), no. 1, 1–24. MR1078211 (92a:05031) ↑1, 6, 10, 24, 26
- [EH95] ———, *The automorphism group of the combinatorial geometry of an algebraically closed field*, J. London Math. Soc. (2) **52** (1995), no. 2, 209–225. MR1356137 (97f:51012) ↑2, 6, 7, 10, 24, 26
- [EM11] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*, American Journal of Mathematics **133** (2011), no. 6, 1503–1532, available at <http://www.arxiv.org/abs/0809.2166>. ↑34, 35, 36, 38
- [EM15] ———, *Galois Groups and Cohomological Functors*, Trans. Amer. Math. Soc. (to appear) (2015), available at <http://arxiv.org/abs/1103.1508>. ↑34, 36
- [EP05] A. J. Engler and A. Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005. MR2183496 (2007a:12005) ↑31
- [FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, third edition, Vol. 11, Springer, 2008. ↑18

- [Gis08] J. Gismatullin, *Combinatorial geometries of field extensions*, Bull. Lond. Math. Soc. **40** (2008), no. 5, 789–800. MR2439644 (2009h:03049) ↑2, 6, 10, 24, 26
- [GS06] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. MR2266528 (2007k:16033) ↑10, 11, 38
- [Lab67] J. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106–132. MR0210788 (35 #1674) ↑34
- [Lan72] S. Lang, *Introduction to algebraic geometry*, Vol. 109, Addison-Wesley Reading, Mass., 1972. ↑21
- [MS82] A. S. Merkurjev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136. ↑10, 34, 37, 38, 39
- [NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Second, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 (2008m:11223) ↑34, 36, 37
- [Pop10] F. Pop, *Pro- $\ell$  abelian-by-central Galois theory of prime divisors*, Israel J. Math. **180** (2010), 43–68. MR2735055 (2012a:12010) ↑4, 6
- [Pop11] ———,  *$\mathbb{Z}/\ell$  abelian-by-central Galois theory of prime divisors*, The arithmetic of fundamental groups: Pia 2010, 2011, pp. 225–244. ↑6
- [Pop12a] ———, *On the birational anabelian program initiated by Bogomolov I*, Invent. Math. **187** (2012), no. 3, 511–533. MR2891876 ↑2, 3, 4, 7, 20
- [Pop12b] ———, *Recovering function fields from their decomposition graphs*, Number theory, analysis and geometry, 2012, pp. 519–594. MR2867932 ↑3, 4, 6, 7, 17, 20
- [Ros98] M. Rost, *Chain lemma for splitting fields of symbols*, Preprint (1998), available at <http://www.math.uni-bielefeld.de/~rost/chain-lemma.html>. ↑9, 16, 34
- [Ser02] J.-P. Serre, *Galois cohomology. Transl. from the French by Patrick Ion. 2nd printing.*, 2nd printing, Berlin: Springer, 2002 (English). ↑16
- [Top14a] A. Topaz, *Commuting-liftable subgroups of Galois groups II*, J. Reine angew. Math. (to appear) (2014), available at <http://www.arxiv.org/abs/1208.0583>. ↑6
- [Top14b] ———, *Detecting valuations using small Galois groups*, Valuation theory in interaction, 2014, pp. 566–578. ↑6
- [Top15] ———, *Abelian-by-Central Galois groups of fields I: a formal description*, Trans. Amer. Math. Soc. (to appear) (2015), available at <http://arxiv.org/abs/1310.5613>. ↑34, 35, 36, 37, 38
- [Voe11] V. Voevodsky, *On motivic cohomology with  $\mathbb{Z}/\ell$ -coefficients.*, Ann. Math. (2) **174** (2011), no. 1, 401–438 (English). ↑9, 16, 34
- [Wei09] C. Weibel, *The norm residue isomorphism theorem.*, J. Topol. **2** (2009), no. 2, 346–372 (English). ↑9, 16, 34

ADAM TOPAZ  
 DEPARTMENT OF MATHEMATICS  
 UNIVERSITY OF CALIFORNIA, BERKELEY  
 970 EVANS HALL #3840  
 BERKELEY, CA. 94720-3840  
 USA  
*E-mail address:* atopaz@math.berkeley.edu  
*URL:* <http://math.berkeley.edu/~atopaz>